2006/2007 : Report 5

OFFICE OF THE
Auditor General
of British Columbia

Audit of Government's Corporate Accounting System: Part 2

December 2006

2006/2007 : Report 5

OFFICE OF THE

Auditor General of British Columbia

Audit of Government's Corporate Accounting System: Part 2

December 2006

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

Audit of government's corporate accounting system (CAS) : Part 2 / Office of the Auditor General of British Columbia. -- [Victoria, B.C.] : Office of the Auditor General of British Columbia, 2006.

(Report ; 2006/2007: 5)

Running title: 2006/2007 report 5 : audit of government's corporate accounting system (CAS): Part 2.

Part 1 published under title: audit of the government's corporate accounting system: Part 1.

ISBN 0-7726-5595-2

1. Corporate Accounting System (Computer system). 2. Finance, Public - British Columbia – Accounting - Data processing - Evaluation. 3. Administrative agencies – British Columbia – Accounting – Data processing – Evaluation. I. Title. II. Title: Audit of the government's Corporate Accounting System. III. Title: 2006/2007 report 5 : audit of government's corporate accounting system (CAS): Part 2. IV. Title: audit of the government's corporate accounting system: Part 1. V. Series: British Columbia. Office of the Auditor General. Report ; 2006/2007: 4.

HJ9921.Z9B74 2006 352.4'309711 C2006-960144-5

OFFICE OF THE
Auditor General
of British Columbia

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m.—4:30 p.m.

TELEPHONE:
250 387–6803
Toll free through Enquiry BC at: 1 800 663–7867
In Vancouver dial 660–2421

FAX: 250 387–1230

E-MAIL: bcauditor@bcauditor.com

WEBSITE:
This report and others are available at our Website, which also contains further information about the Office: http://www.bcauditor.com

REPRODUCING:
Information presented here is the intellectual property of the Auditor General of British Columbia and is copyright protected in right of the Crown. We invite readers to reproduce any material, asking only that they credit our Office with authorship when any information, results or recommendations are used.

2007-02211/

OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250 387-6803
Facsimile: 250 387-1230
Website: http://bcauditor.com

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my Office's 2006/2007 Report 5: Audit of Government's Corporate Accounting System: Part 2.

Arn van Iersel, CGA
Auditor General (Acting)

Victoria, British Columbia
December 2006

copy: Mr. E. George MacMinn, Q.C.
Clerk of the Legislative Assembly

Table of Contents

Deputy Auditor General's Comments 1
A strong control environment is important 1
Our audit focus 2
Conclusion 3
Key Findings 3
Our recommendations 6
Detailed Report 11
Background 11
The control environment 12
This type of computing system carries with it additional business risks 14
Our audit focus 16
Security administration controls 19
What we examined 21
Conclusion 22
Main findings 23
General ledger controls 29
What we examined 31
Conclusion 32
Main Findings 32
Supplier maintenance controls 45
What we examined 46
Conclusion 47
Main findings 48
Purchasing and accounts payable controls 61
What we examined 64
Conclusion 65
Main findings 67
Response from the Ministry of Finance and the Ministry of Labour and Citizens' Services ... 77
Appendices 99
Appendix A: History of Changes to Government's Corporate Accounting System (CAS) 101
Appendix B: Summary of Recommendations 103
Appendix C: Office of the Auditor General: 2006/2007 Reports Issued to Date 113

Acknowledgements

Audit Team

Bill Gilhooly

Pam Hamilton

Faye Fletcher

Ada Chiang

David Lau

In British Columbia, all government ministries, numerous agencies and many of the independent offices of the Legislature enter their financial information into one central accounting and financial reporting system, the Corporate Accounting System (CAS). This means that all transactions are recorded, processed and accessible on the one integrated system. CAS is the largest central accounting system in the province.

By connecting to the shared government network, about 24,000 users (mainly government employees) have access to CAS from offices throughout British Columbia. All government expenses and revenue—about $27 billion and $29 billion, respectively, in 2005/2006—are processed through this system. This represents more than 4 million expenditure transactions, more than 2 million balance sheet transactions and about 620,000 revenue transactions. As well, more than 275,000 individuals and businesses are listed in the system, as suppliers that could receive payments from government for goods or services.

Transactions initiated from locations across the province are recorded as accounting entries, such as payments made and revenue collected. In turn, these transactions are used to generate reports that help management monitor spending levels and make business decisions. And, once summarized, these transactions are used to produce government's financial statements.

A strong control environment is important

Faulty entries into CAS—say, because of human error or unauthorized access to the system—could result in incorrect or unauthorized payments, as well as critical business functions (such as financial reporting) being seriously compromised. Furthermore, system maintenance problems or a lack of processing capacity could prevent government staff from accessing CAS, resulting in processing disruptions.

The potential for these problems is not unique to CAS. Every computing system faces similar risks. Any operating system could fail to meet current or future business requirements, resulting in performance or availability problems. Unauthorized changes could be made to an operating system, affecting security, availability or performance. Someone could gain unauthorized access and view, or change, the information in the accounting system. Or the facility

that houses the system could be compromised by unauthorized access or a disaster, leading to system unavailability or the loss of information.

The only way to minimize these risks (and to maximize the likelihood of detecting problems if they do occur) is through a strong control environment. Properly positioned controls contribute to the reliability and accuracy of the financial information. They ensure that the risk of fraud and errors is reduced.

It is management's responsibility to see that controls, both computerized and manual, are in place and operating properly to promote compliance with an organization's policies and regulations and to lessen any foreseeable risks to business processes.

Our audit focus

This audit was part of a series we undertook to evaluate controls in the CAS computing environment. Since its initiation in April 2001, government has been implementing and enhancing the system in stages. The Office's approach has therefore been to conduct a series of audits over several years to keep pace with these changes.

In our 2005 report *Audit of the Government's Corporate Accounting System: Part 1*, we presented our findings on controls over the governance of CAS and the CAS operating system and central database.

This report, *Part 2*, covers our audit of the CAS application in the following areas—the administration of security over access to the accounting software, and certain controls over two significant components of the accounting software: the general ledger module and the purchasing/accounts payable modules. A lack of proper controls in these areas could significantly affect the reliability of government's financial information.

In these key areas, we examined the controls in place designed to ensure: (1) access to the system and to specific activities was appropriately restricted; (2) transaction processing in the general ledger module was complete, accurate, and timely; and (3) transactions in the purchasing/accounts payable modules were valid.

Conclusion

We concluded that, with some exceptions, proper control procedures were in place and being followed to ensure that financial information is processed completely, accurately and on a timely basis. However, we identified several key areas where we felt that controls were not adequate to address the risk of incorrect or fraudulent payments.

Key Findings

Incorrect access to the accounting system could jeopardize its integrity

Control over who has access to the accounting system and at what level is a shared responsibility between Corporate Accounting Services and the ministries. For the most part, security is being well managed, but ongoing maintenance is a concern. There were many incorrect access assignments on the system as a result of users changing ministries, job functions or job status and their access rights not being adjusted accordingly.

This problem is a consequence of both a lack of timely communication by the ministries to Corporate Accounting Services, and regular monitoring by Corporate Accounting Services to promote compliance.

There is a risk of inaccurate chart of accounts coding and consequently inaccurate financial reporting

General ledger information is used to produce government's financial statements and financial reports for management. The chart of accounts maps out how this information will be classified, rolled up and summarized to produce the financial statements and reports. If records in the chart of accounts are not correct, it could result in inaccurate reporting.

In the case of chart of accounts maintenance, there is a risk of unauthorized changes to chart information. Also of concern was the lack of procedures for monitoring chart data to ensure it is current and relevant.

Deputy Auditor General's Comments

Payments could be directed to incorrect suppliers

The supplier master data is a central component within Oracle Financials that impacts purchasing and accounts payable transaction processing. It contains supplier information such as addresses and bank accounts used for directing payments. Usually each individual supplier is issued a unique number that is associated with their address and bank account. In the previous accounting system there was a limit on the number of unique supplier records that could be issued. To work around this limitation "generic" suppliers were set up. Although the current system does not have the same restriction, the generic suppliers still exist as such in the new system.

These "generic" suppliers have been set up in such a way that one supplier record is associated to multiple suppliers. These suppliers have the same last name, first initial and supplier number, and the only way to uniquely identify them is by their address. If the correct addresses are not specifically selected during invoice processing, there is a risk that cheques could inadvertently be sent to the wrong address and potentially even cashed by the recipients, since they have the same name as the payee.

Payments to some suppliers are not fully reported in government's financial statements

A block supplier category is used for recording payments (often one-time payments) to multiple payees—without each payee having to be set up as a supplier. For example, block suppliers are used for paying scholarships to students through universities and colleges.

Total amounts paid to each supplier receiving more than $25,000 in a fiscal year are reported in a supplementary schedule to the government's financial statements. Suppliers paid through the block supplier category are not reported. We are concerned that some of these payments should be included and therefore there is a risk of non-compliance with government's reporting requirements.

Deputy Auditor General's Comments

Electronic payments could be directed to fraudulent suppliers

Weaknesses in the way bank account change requests are handled are putting the validity, accuracy and completeness of supplier information at risk. There are insufficient controls in place in ministries to verify that suppliers requesting the changes are in fact legitimate. Unless individuals or organizations providing the bank account information are verified to have the authority to do so, there is a risk that payments could be redirected from existing suppliers' bank accounts to fraudulent ones.

There is also no monitoring in place to ensure that all supplier linkages to bank accounts are valid. When links from suppliers to bank accounts are made, payments are automatically directed to the linked bank accounts. If the links were incorrect due to error or fraud, the payments would be deposited to incorrect bank accounts.

There is opportunity for unauthorized transactions

Accountability and responsibility for spending public money is placed on ministers and deputy ministers. In order for them to carry out their responsibilities, they have delegated their financial signing authority to ministry officials, referred to as "expense authorities".

Generally, purchase transactions appear to be adequately reviewed by expense authorities to ensure the validity of the transactions. However, in our review of the electronic procurement process, two key concerns were identified. We are concerned about the ability to make one-time address changes, redirecting suppliers' cheques to different addresses, perhaps fraudulent ones. Also of concern is the ability of expense authorities to approve purchases without knowing who the suppliers will be. This could result in procuring goods and services from inappropriate suppliers which may contravene government's procurement standards.

Monitoring procedures are not sufficient to detect errors or fraud in ministry expenses

The expense authorities' review of the financial management reports is an important control for monitoring expenditures. We are satisfied that this was being carried out but the effectiveness of the review could be improved. Each level of review could potentially detect different conditions resulting from different risks. For example, the risk that expense authorities or CAS support staff with full system access enter fraudulent transactions could

be mitigated with various levels of monitoring. For monitoring to be effective in detecting such transactions, the risks must be understood by those responsible for the reviews. However, expense authorities and the managers responsible for monitoring were not sufficiently aware of the risks that their reviews were supposed to be monitoring.

Our recommendations

The following outlines the key improvements needed. We recommend that:

- Corporate Accounting Services take a more proactive role in ensuring all access is appropriate by alerting ministries of possible problems with user access.
- procedures be established to communicate staff changes to security administrators in a timely manner to ensure effective user access change management, and to periodically review user access levels to ensure access granted remains appropriate based on users' positions.
- monitoring activities be formalized and carried out by the Office of the Comptroller General (OCG) to ensure the chart data remains current and relevant.
- Corporate Accounting Services establish formal policies restricting further set-up of generic suppliers and formalize a plan to establish a well-defined approach for using, managing and updating existing generic supplier records.
- OCG establish clear criteria for monitoring and compliance activities to ensure that the block supplier data remains current and relevant.
- policies and procedures be established to define clearly a ministry's role and responsibilities in the bank account maintenance process, and to govern the extent of ministry review required for ensuring the completeness and accuracy of banking information obtained.
- OCG effectively communicate to ministries the risks associated with banking activities and advise them how to detect the potential threats and to ensure that controls are functioning properly to address them.

- management at Corporate Accounting Services formalize procedures to monitor all supplier linkages to bank accounts and compare the details of the reported activities to source documents to ensure there are no unauthorized or inappropriate bank account linkages.
- Corporate Accounting Services explore the feasibility of requiring approval from expense authorities when manual changes are made to suppliers' cheque mailing addresses to prevent unauthorized changes. Guidance should also be established to ensure proper validation procedures are carried out when approving these changes.
- management require expense authorities to review procurement transactions when supplier information is subsequently added to purchase orders or changed, to ensure the appropriateness of the suppliers used for procuring the goods and services.
- OCG take on the initial responsibility of effectively communicating with ministries the risks of potential fraud in purchase and accounts payable transactions and advising them on how to detect potential threats resulting from these risks.

In the following "Detailed Report" we have identified other areas where controls should be strengthened. Appendix B lists all recommendations made to address issues raised in our audit. I am pleased to note that many of these recommendations have been or are being addressed by management.

I wish to thank those who assisted and cooperated with our Office in gathering information for the audit. As well, I would like to acknowledge the hard work, professionalism and dedication of Office staff in the production of this report.

Errol S. Price, CA, CMC
Deputy Auditor General

Victoria, British Columbia
December 2006

Detailed Report

The main component of CAS is the Oracle Financials Accounting System (referred to here as Oracle Financials). It runs on a UNIX operating system, using an Oracle database. This computing environment is shown in Exhibit 1.

Common IT Services (CITS), a part of the Ministry of Labour and Citizens' Services, owns and is responsible for the hardware and related operating system software on which the Oracle Financials application runs. (Note: In June 2006, CITS changed its name to Workplace Technology Services.) Ministry and agency staff can, by logging on individually with a unique government username and a password, access Oracle Financials through a web browser on the shared government network.

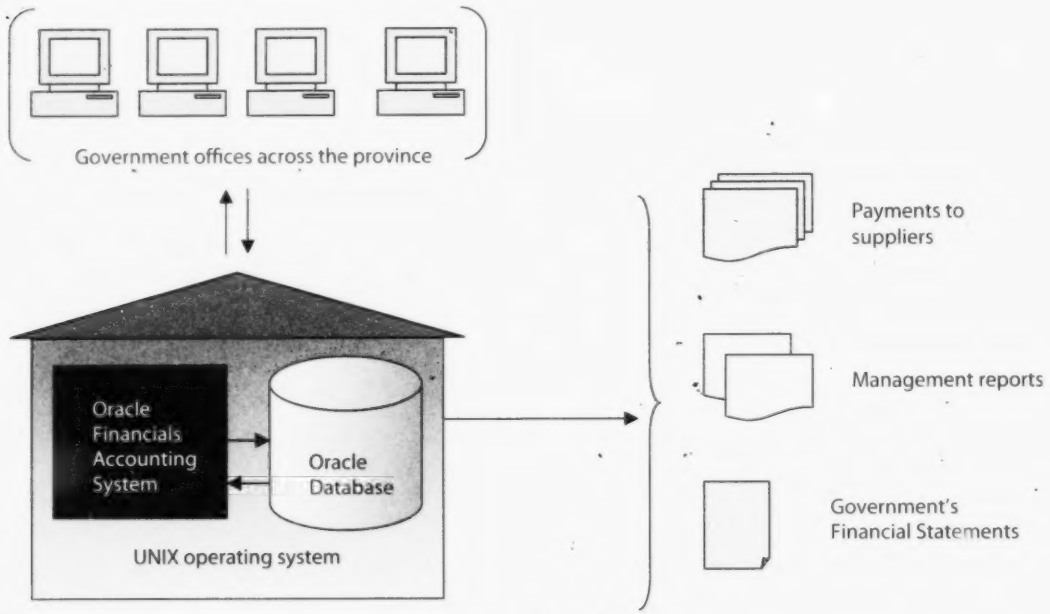
Corporate Accounting Services (also part of the Ministry of Labour and Citizens' Services) owns the Oracle Financials and Oracle database software and is responsible for its licensing. They work with CITS to provide maintenance, security, capacity planning, back-up and recovery for Oracle Financials, the UNIX operating system and the Oracle database. Corporate Accounting Services is also responsible for the delivery of the financial system and providing support to all ministries and other government agencies.

The Office of the Comptroller General (OCG) has overall responsibility for the central accounts of government and the approval of ministry financial organizational structures. The Office is also responsible for the financial management and administration policy and procedures used by ministries. Reliance is placed on ministry staff to follow the policies and procedures set by OCG when carrying out their daily tasks, such as creating or changing account structures and entering transactions into CAS, for instance purchases and journal entries.

Background

Exhibit 1

A simplified look at the CAS computing environment



Transactions, initiated from locations across the province, are used to generate reports that help management monitor spending levels and make business decisions. And, once summarized, these transactions are used to produce government's financial statements.

The sound operation of many of government's key business functions therefore depends on:

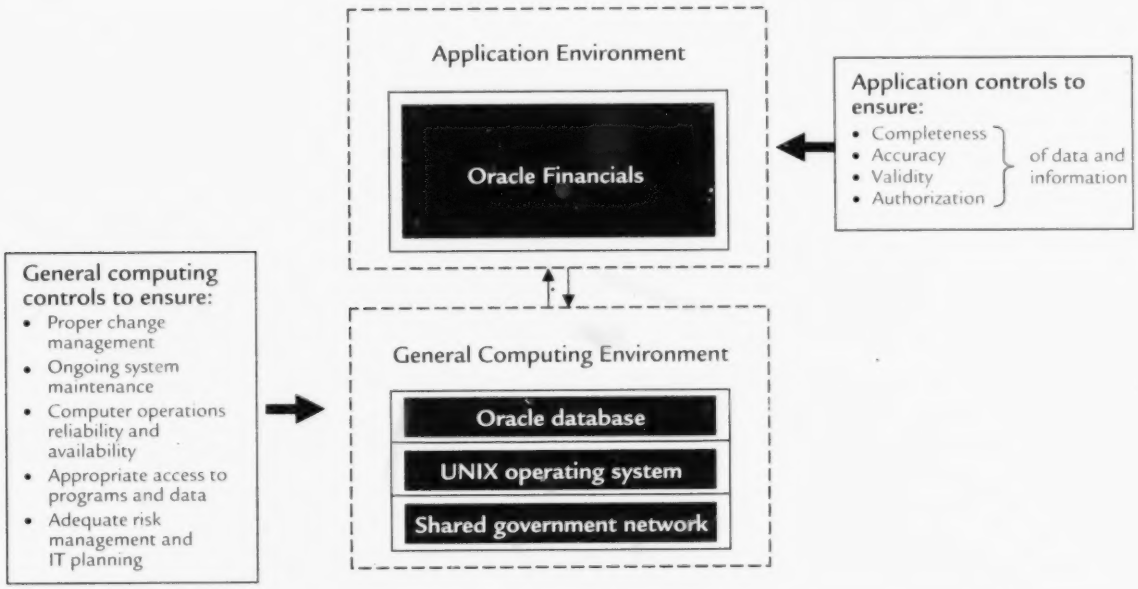
- every transaction entered and processed in CAS being authorized (valid), accurate and complete; and
- the information generated by the system being accurate, complete, timely and continuously available.

The control environment

The CAS computing environment can be conceptually divided into two main parts (Exhibit 2): the general computing environment (the Oracle database, UNIX operating system, and shared government network) and the application environment (Oracle Financials).

Exhibit 2

CAS control environment

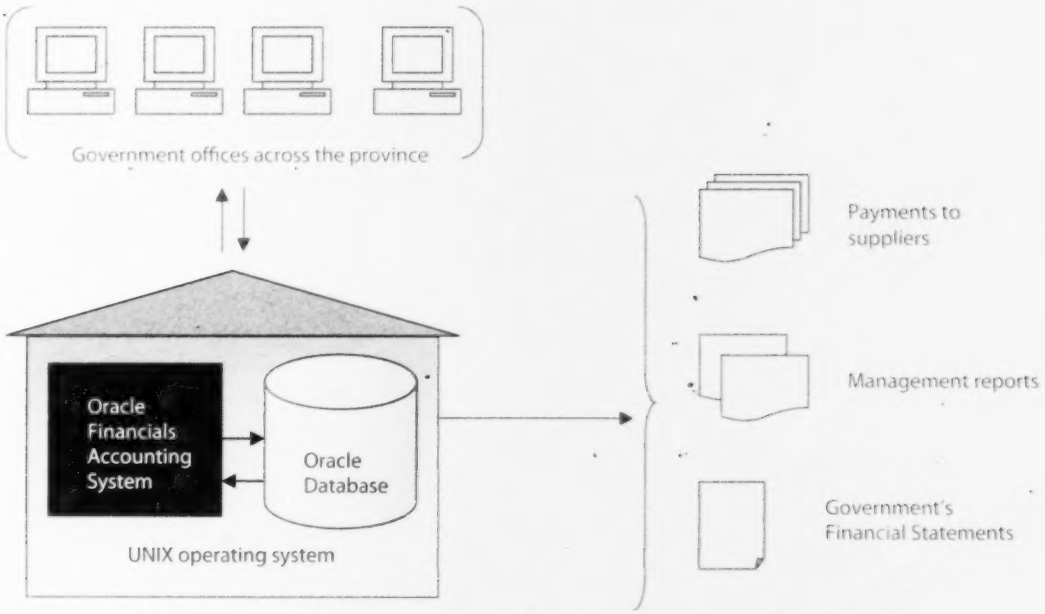


The reliability of CAS depends on having appropriate computerized and manual controls over:

- the general computing environment, to ensure that the system is reliable, secure and available for processing. Such controls include: segregation of incompatible duties; assurance of compliance with proper change management processes; appropriate restriction of access to programs and data; performance monitoring; regular back-up and recovery; and adequate physical security.
- the application environment, to ensure that only authorized data is recorded and processed correctly to produce valid results. Such controls include: edit checks; running of exception and balancing reports; segregation of incompatible functions; manual procedures performed by management and staff; and computer processes in the application that initiate, approve and match data, as well as ensuring that data is correctly processed, posted and stored.

Exhibit 1

A simplified look at the CAS computing environment



Transactions, initiated from locations across the province, are used to generate reports that help management monitor spending levels and make business decisions. And, once summarized, these transactions are used to produce government's financial statements.

The sound operation of many of government's key business functions therefore depends on:

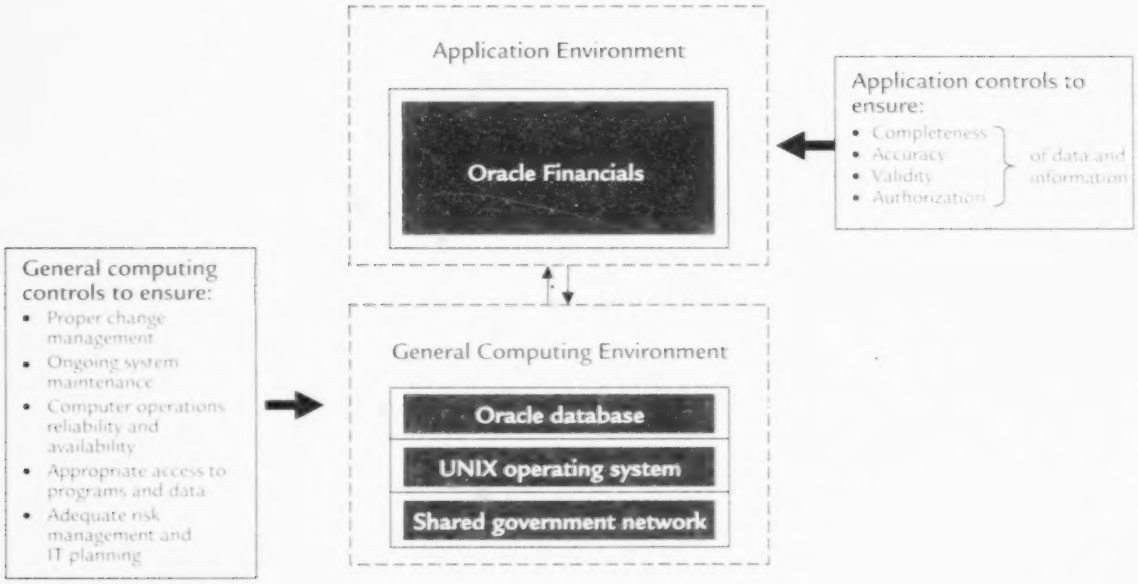
- every transaction entered and processed in CAS being authorized (valid), accurate and complete; and
- the information generated by the system being accurate, complete, timely and continuously available.

The control environment

The CAS computing environment can be conceptually divided into two main parts (Exhibit 2): the general computing environment (the Oracle database, UNIX operating system, and shared government network) and the application environment (Oracle Financials).

Exhibit 2

CAS control environment



The reliability of CAS depends on having appropriate computerized and manual controls over:

- the general computing environment, to ensure that the system is reliable, secure and available for processing. Such controls include: segregation of incompatible duties; assurance of compliance with proper change management processes; appropriate restriction of access to programs and data; performance monitoring; regular back-up and recovery; and adequate physical security.
- the application environment, to ensure that only authorized data is recorded and processed correctly to produce valid results. Such controls include: edit checks; running of exception and balancing reports; segregation of incompatible functions; manual procedures performed by management and staff; and computer processes in the application that initiate, approve and match data, as well as ensuring that data is correctly processed, posted and stored.

The adequacy of controls over both of these key parts of CAS directly affects the reliability and integrity of government's entire accounting service and its financial reporting. For this reason, a strong control environment is imperative.

This type of computing system carries with it additional business risks

Oracle Financials is what is known as an enterprise resource planning (ERP) software application. An ERP application integrates departments and functions across an organization by taking common financial activities (such as purchasing, receiving, accounts payable, and payments) and processing all the related transactions on a single computer system.[1]

All transactions entered by ministries into Oracle Financials are recorded in the Oracle database in thousands of data tables. In most cases, this database is updated simultaneously with every transaction entered online. Oracle Financials is a modular system. This means that each module (see Exhibit 3) transfers information about an entered transaction to other associated modules. For example, an entry to purchase goods will create entries in the accounts payable module (a financial expenditure business process) and the general ledger module (a financial accounting business process). So, if the initial entry is invalid, inaccurate or incomplete, several business functions can be invalid, inaccurate or incomplete—if the error is not detected by system controls prior to processing.

[1] In the past, organizations typically had three separate systems: one to handle purchasing, one to record accounts payable and one to record payments. Before CAS was implemented by the province, a variety of computer systems for financial management existed across the organization: some ministries had online access to enter transactions; others had to process transactions through a central batching system.

Exhibit 3

Modules used in government's accounting system

Accounts Payable – used to enter, validate and authorize payment of supplier invoices and employee expenses.

Accounts Receivable – used to record all aspects of an accounts receivable business process, including: entering customers, entering accounts receivable transactions, producing invoices, and recording the payments.

Budget and Chart of Accounts – provides a common system for government staff to build and maintain their budgets and to build and maintain their Chart of Accounts and post them to the general ledger.

Fixed Assets – used to enter and maintain information about capital and attractive assets, including both purchased and "construction in process" assets. Asset maintenance includes the transfer, retirement and disposal of assets, as well as the calculation of depreciation, calculation of gains and losses, and capitalization of purchased assets.

General Ledger – a complete financial management system for provincial government ministries. The general ledger is updated from all sub-systems (accounts payable, accounts receivable, fixed assets and purchasing) and from the CAS Generic Interface. It is also updated instantly online for all manually entered and posted journals.

iExpenses Self-Service – a web portal to the accounts payable module. Employees use it to enter their travel expense claims and submit these for approval by the appropriate expense authority.

iProcurement Self-Service – a web front-end to the purchasing module, providing staff with the ability to requisition services or supplies, based on spending limits, and receive goods and services.

Purchasing – used to track/record purchase instruments such as purchase orders, contracts and letters of agreement. Each purchase instrument generates an encumbrance against the general ledger.

Source: CAS website www.cas.gov.bc.ca

To ensure the integrity of information entered into this ERP system, Oracle Financials is highly dependent on four basic types of controls:

1. **manual controls** — management controls such as report monitoring and manual reconciliations and approvals,
2. **inherent controls** — controls built into the operation of the system, such as edit and validation routines,
3. **configuration settings** — customized options to control and direct processing operations, and
4. **logical access security** — restrictions on access to system functions.

The effectiveness of these controls is important because in Oracle Financials, as in any ERP system, there are business risks that arise:

- A single point of failure could occur because all government financial information and processing is now within one system rather than several;

Background

- Incorrect information could be accessed in real time, if attention is not paid to the controls over information at the front-end of the system (the point of entry of the information) along with the controls at the back-end (the financial processes); and
- Because of reliance on online, real-time information, government's business could be interrupted if problems are not quickly dealt with to maintain a continuously available processing environment.

To respond to these risks, it is management's responsibility to ensure that effective controls, both computerized and manual, are in place.

Oracle Financials does have some built-in, automated features to ensure data entered meets predefined criteria. One example is the use of edit routines, such as matching the purchase order totals to invoice totals to validate invoices for payment. Nevertheless, because many of these features can be pre-configured in Oracle Financials—meaning that previously set parameters can be reset—it is critical that proper manual controls, such as change management and security policies and procedures be in place.

Our audit focus

The province has been implementing and enhancing CAS in stages (see Appendix A). The CAS environment has continued to improve, with new functions and hardware being added and existing hardware and software being upgraded. Our approach has therefore been to conduct a series of audits over several years to keep pace with these changes.

Our first step, in the spring of 2002, was to assess controls in UNIX. We next assessed the controls related to the Oracle database, in the fall of 2003. Corporate Accounting Services acted on many of the recommendations we made concerning each of these system components. Then, in the winter of 2004, we carried out a follow-up review to examine government's progress in implementing our recommendations. At the same time, we looked at what governance controls were in place to ensure the CAS environment was able to provide for continuous and effective delivery of service.

Background

In the audit reported here, we assessed the controls in the application environment, directly related to security administration, general ledger transactions and access to and authorization for purchasing and accounts payable transactions.

Our examination focused on controls over business processes related to:

— **security administration**
- management of user access,
- management of access to information and activities, and
- maintenance of security control settings.

— **financial accounting (the general ledger module)**
- chart of accounts maintenance,
- journal processing, and
- reconciliation and financial reporting.

— **financial expenditure (the iProcurement, purchasing, and accounts payable modules)**
- supplier maintenance, and
- management of approval levels and authority over purchases and payments.

During our audit, we worked with staff from the Office of the Comptroller General, Corporate Accounting Services and several ministries.

Audit criteria

Our audit was based on criteria set out in the *Information Technology Control Guidelines* (3rd edition) published by The Canadian Institute of Chartered Accountants, and *Security, Audit and Control Features—Oracle Applications* issued by the IT Governance Institute.

The *Information Technology Control Guidelines* provide standard control objectives used by Certified Information Systems Auditor specialists in Canada when they carry out examinations of the integrity of information and information systems. The objectives describe the actions, roles and accountabilities that those who manage and use information technology are expected to take to manage the associated risks.

Background

Security, Audit and Control Features - Oracle Applications is a technical and risk management reference guide specifically for the Oracle Financials system. The IT Governance Institute provides this guidance to help management and assurance professionals understand the risk and manage the security, audit and control features of Oracle Financials.

We took a risk-based approach in our work, first identifying the significant risks, then determining what key controls were in place, and finally testing these controls to confirm their adequacy and existence. Testing the latter involved interviews, observation, review of supporting documentation, and verification of table data using audit software tools.

We performed our audit in accordance with the assurance standards recommended by The Canadian Institute of Chartered Accountants and accordingly included such tests and other procedures we considered necessary to obtain sufficient evidence to support our conclusions.

It is important to note that any system of internal control has inherent limitations. This means that despite the control procedures in place, errors or irregularities may still occur and go undetected. Furthermore, evaluating a system's reliability in future periods is subject to the risk of procedures becoming inadequate as conditions change or procedures not being complied with.

Security Administration Controls

Security administration is about controlling access to the system—ensuring that only those authorized can gain access to the system, and that those authorizations are monitored. If security within and around CAS is not properly administered, there is a potential that government employees and others could inappropriately access sensitive and confidential information, change existing records for payments to suppliers or add fraudulent new ones.

In general, security over the government's accounting system is well managed, but there are several areas where controls over access could be improved.

Oracle Financials is controlled by the use of responsibility assignments—which grant users access privileges to perform specific functions and access required data. It can be thought of simply like a set of keys to an office building. Some doors can be opened, others cannot. All users will have the key to the front door, but beyond that access is restricted. Users must enter their unique username and password to sign on to the system, where they are then connected to their set of keys—or "responsibility." This access is further restricted by profiles and data security rules.

There are three levels of security administration:

- Oracle Financials provides the overall structure for security and defines responsibilities that would fit organizational roles. CAS security administrators use these predefined responsibilities and customize them to suit government's needs.
- Ministry security administrators request new user accounts and responsibilities from CAS support staff.
- CAS support staff enable and disable users, assign and remove responsibilities upon the request of ministry management, and reset passwords.

Security Administration Controls

Large systems, regardless of the controls in place, usually have some predictable key risk areas related to security administration. We have selected the following five key risk areas for evaluation:

1. The risk that controls built into the system may not be used, resulting in a system that is less secure than it could be. For example, there are controls that can be set within the software:
   - To make it more difficult to guess passwords, the system can require users' passwords to be complex—such as using combinations of alpha, numeric and capitals—and require passwords to be reset every specified number of days.
   - To decrease opportunities for unauthorized use of the system during non-business hours, the system can deny access to users at night or over the weekend.
   - To prevent unauthorized access when staff are away from their work areas during the day, the system can require userids and passwords to be re-entered if sessions have been inactive for a predetermined period of time.
2. The risk that users could be granted access beyond what they require to perform their day-to-day duties. This could result in inappropriate access to sensitive or confidential information (such as bank accounts), even though access to such information is not required.
3. The risk that ex-employees or contractors, or those that have assumed new positions could still have the same access to the corporate accounting system. Either situation could result in unauthorized modifications being made or inappropriate access being granted to sensitive or confidential information.
4. The risk that poor monitoring of access to key information (such as bank accounts) or of the activities of staff with potential for unlimited access could allow fraudulent activity to go undetected or prevent later follow-up.
5. The risk that access to government's accounting system could be jeopardized, if management of the underlying Oracle ministry userids is not kept up to date.

Security Administration Controls

On May 31, 2004, single sign-on to CAS was implemented, allowing users to access Oracle Financials with the same unique usernames and passwords that gives them access to the government network. This was done to simplify access for authorized users to the various applications delivered and supported by CAS. Each user need only remember one username and one password (their government password)—an additional Oracle Financials password is created automatically in the background, encrypted for security and internally linked to their government userid.

Although it is more efficient for users to use a single sign-on process, there is a risk that some users would have excessive and unauthorized access if the underlying Oracle Financials usernames that are linked to the government ones do not have the correct and current access.

How serious a risk is this? When single sign-on for CAS was implemented in 2004, a cross-government username clean-up was initiated. During that process, a few thousand usernames were found to have access that was not required, even though CAS had been operational for less than five years. Ministries should have been notifying Corporate Accounting Services of employee, and therefore user, changes on a routine basis. We are not satisfied that the risk of this happening again has been adequately addressed within the current process.

What we examined

We tested the control procedures designed to reduce the identified risks, and to ensure the control objectives were met.

Control objectives for security administration

We expected to find that:

- Oracle Financials security and control settings are adequately defined;
- the security administration function is defined and assigned and security administration policies and procedures exist to ensure adequate change management of user access;
- access to data is appropriately restricted and monitored;
- users only perform compatible functions;
- system profiles are adequately defined, access to them is restricted and changes are monitored; and
- access to system output is appropriately restricted.

Security Administration Controls

We checked:

- what built-in system controls were being used;
- how the security administration function was set up and whether it is effective;
- who has access to what information and at what level, and whether those users were required to have that access for business purposes;
- how a user is initially set up to access the system and how changes in access requirements are communicated and dealt with; and
- what monitoring is being done to ensure that access to high-risk information and activities is only done when required for business purposes.

Conclusion

For the most part, security is well managed, but there are several areas where controls should be improved. The main problem is the potential for incorrect access to the system because of users changing ministries, job functions or job status without their access being adjusted as well. This condition is a consequence of both a lack of, or untimely, communication by the ministries to Corporate Accounting Services and a lack of regular monitoring to promote compliance.

Certain functions that key support staff must have also give them the ability to gain unlimited access. This continues to be a concern that must be monitored carefully by Corporate Accounting Services and ministries. Corporate Accounting Services has made progress in the area of internal monitoring over the past year. This, combined with ministry controls designed to review the validity and accuracy of transactions, will mitigate the risk of fraudulent activity.

In some cases, ministry and CAS support staff have retained access to sensitive or confidential information they no longer require for business purposes. In addition to system exception reports run by Corporate Accounting Services to identify access problems, a notification system of access changes that need to be made both internally at Corporate Accounting Services and in the ministries could greatly decrease problems with excessive system access.

The recommendations concerning security administration controls are listed in Appendix B.

Security Administration Controls

Main findings

Ensuring Oracle Financials security and control settings are adequately defined

Login access

The majority of users enter Oracle Financials through a single sign-on process using their unique government userid and password. Controls over these userids and passwords are maintained within IDIR (the BC Government Employee userid directory). We found that requirements for password strength, length and expiry comply with government's Information Technology Security Policy.

However, a number of users and support staff are allowed to login directly to the accounting system, bypassing the single sign-on process. We recommend that a review be performed to determine whether these users and support staff require this access; and for those that do require it, security features—such as using more complex passwords and setting password expiry dates—be adopted.

Controlling access to activities

Access to Oracle Financials is controlled by assigning responsibilities to users. Each responsibility enables access to specific functions, allowing users to only perform certain activities.

We reviewed the appropriateness of functions assigned to certain responsibilities related to general ledger, purchasing and accounts payable activities. For example, some responsibilities allow users to create changes and update the supplier file, while others allow users to enter supplier invoices in the accounts payable module.

We found that the functions assigned to the responsibilities examined were generally appropriate and consistent with their respective business requirements.

Controlling access by assigning "responsibilities"

Oracle Financials is controlled by the use of responsibility assignments which grant users access privileges to perform specific functions and access required data. This means that when users sign on to Oracle Financials using a particular responsibility, they are only granted access to perform particular activities. Responsibilities should only be assigned to users when it is appropriate for their job requirements.

Therefore, controlling access to activities in the system depends on ensuring that (1) the functions assigned to responsibilities are correct and appropriate, and (2) responsibilities are assigned only to those users who need that access to do their job.

The Oracle-supplied responsibilities (as configured "out-of-the-box") provide users with maximum access to the module's functions. Therefore, to limit access by job role, each responsibility requires customization to remove functions that are not permitted or needed.

Ensuring the security administration function is defined and assigned, and security administration policies and procedures exist to ensure adequate change management of user access

Security administration function

We found that the security administration function is generally defined and assigned, however we noted the following concerns:

Security Officer role

The authority of the new Security Officer position at Corporate Accounting Services has not yet been clearly defined, which could decrease the effectiveness of the position.

Security initiatives typically increase a department's budget without providing a production gain. Therefore, these initiatives may not be accepted unless senior management proactively supports the position and provides the authority to make acceptance a requirement. We recommend that the role of the Security Officer be clearly defined to reflect this authority.

Corporate Accounting Services role

Although the ultimate responsibility for user access lies with each ministry, as it should, Corporate Accounting Services staff have valuable knowledge of CAS and its various tools (such as exception reports) that they could use to alert ministries of possible problems with user access.

Given the problems found in user access, we recommend that Corporate Accounting Services take a more proactive role in ensuring all access is appropriate.

Change management of user access

There were policies and procedures for change management of user access, however we noted several control weaknesses.

User access is centrally administered in ministries and restricted to a few designated staff, who are referred to as ministry security administrators. These individuals have the authority to submit requests to set up new users, inactivate existing users, or change users' access. Corporate Accounting Services administers these changes based on the requests received.

We found that there were not adequate processes for ensuring that Corporate Accounting Services was notified when employees with access to CAS changed job responsibilities.

We noted that formal processes were in place to ensure only authorized users are set up with the appropriate security access, based on job requirements. However, ongoing security access maintenance concerned us. Once access was set up, it was not adequately reviewed or monitored to ensure the responsibility assigned remained current and relevant to the users' job status. This is particularly important in view of certain responsibilities that have powerful functions—such as those that can assign employee approval authority or "force-approve" invoices (i.e., override the normal approval process).

Consequently, we found many cases where individuals no longer working for government (as either employees or contractors) or who have assumed new positions within government have not had their access to the government accounting system changed. This same problem was identified in 2004, when the single sign-on process was implemented and a few thousand userids were removed—these users could have gained unauthorized access, if they had access through the government network. Unauthorized access remains a concern. We recommend that procedures be established to communicate staff changes to security administrators in a timely manner and then to Corporate Accounting Services.

Security Administration Controls

Ensuring access to data is appropriately restricted and monitored

Certain functions that key support staff must have also give them the ability to gain unlimited access. This continues to be a concern that must be monitored carefully by Corporate Accounting Services and the ministries.

Monitoring high-risk activities

We found that responsibilities with access to high-risk functions—such as those that define the origin and type of journal, the set-up of suppliers, and the approval groups and procurement document types—had been appropriately restricted to CAS support staff.

Some types of information (such as bank accounts) have been classified as high risk. Monitoring access to this sensitive information, as well as monitoring the activities of key support staff with potential for unlimited access, could detect fraudulent activity. The same is true for all high-risk activities performed for business purposes: the access of all staff carrying out those activities should be periodically reviewed and monitored as well, to ensure their access is required. We found that Corporate Accounting Services has taken the necessary measures to ensure that high risk activities and data tables are monitored. The identification of sensitive data is an on-going function.

Monitoring failed login attempts

Repeated failed login attempts can indicate unauthorized users are attempting to gain inappropriate access to CAS. Such attempts, we found, are recorded, but not monitored and followed up, and we therefore recommend that the Security Officer perform these tasks.

Ensuring users only perform compatible functions

Users should only be granted the access required to perform their job function. To minimize the risk of inappropriate access, user access should be reviewed periodically to ensure it is still required. During our review of access by staff at Corporate Accounting Services, we found instances where some staff had potential for unlimited access or access to high-risk activities—such as the capability to make a purchase, approve it, receive the goods and make the payment—when it was not a requirement for their job

function. As explained in earlier sections of this report, we also found many instances where the access granted ministry employees did not match their job roles. We recommend that the inappropriate access identified be removed and that procedures be established to periodically review user access levels.

Ensuring system profiles are adequately defined, access to them is restricted and changes are monitored

System profiles are settings that define the way Oracle Financials functions. We found that the profiles tested were set appropriately.

Values issued to certain system settings by CAS support staff have a direct effect on security. Examples include the number of logon attempts that can be made before user access is revoked, and the length of time a logged in session can sit idle before it is automatically ended. Because it is important that any changes to these setting be authorized and that they conform to security policies, we recommend that the Security Officer be consulted when the values issued to security settings are changed.

Ensuring access to system output is appropriately restricted

Reports for individual ministries are generated nightly. We found that procedures in place were reasonable to ensure access to the reports was appropriately restricted.

Controls over the general ledger module are necessary to ensure that all information entered into the general ledger is valid, complete, and accurate, and that the chart of accounts correctly maps how this information should be used to produce accurate and complete government financial statements and financial management reports.

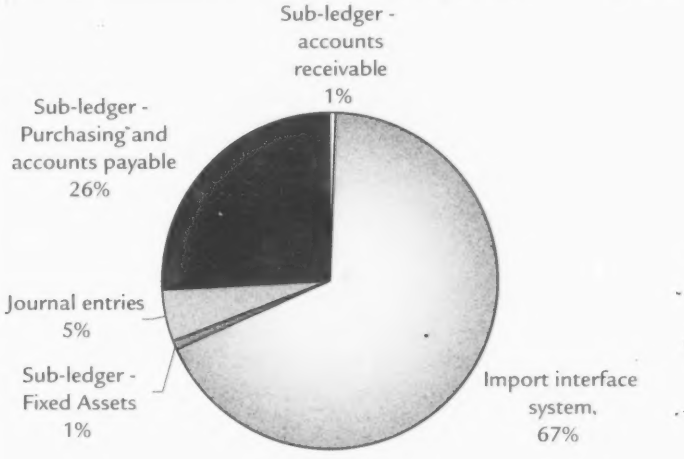
Most of the essential controls over the general ledger are operating as they should, but those intended to prevent unauthorized access and to ensure accuracy should be strengthened to protect the integrity of the data and the financial statements based on that data.

The Oracle Financials general ledger module is the central point for data collection of all financial transactions processed for government ministries and agencies. This single ledger is referred to as the BC Government (BCGOV) "set of books." From this, management generates information for financial reporting and decision-making.

Normally, transactions are entered in one of the following Oracle Financials sub-ledgers: purchasing, accounts payable, accounts receivable, and fixed assets. As shown in Exhibit 4, data in all of these sub-ledgers is then transferred to the Oracle Financials general ledger. Transactions not entered into any of the sub-ledgers can instead be entered directly into the general ledger as journal entries, or imported into Oracle Financials through an interface system.

Exhibit 4

Transactions entered into the general ledger module


Sub-ledger - accounts receivable 1%
Sub-ledger - Purchasing and accounts payable 26%
Journal entries 5%
Sub-ledger - Fixed Assets 1%
Import interface system, 67%

Transactions in the general ledger are from the following sources:

- transactions processed through the Oracle Financials sub-ledgers to the general ledger,
- journal entries entered directly to the general ledger, and
- transactions imported to the general ledger (or through a sub-ledger to the general ledger) from the interface system.

Source: Compiled from 2004/05 transactions extracted from CODE

The three main processes in the financial accounting cycle that we looked at were:

- chart of accounts data maintenance;
- journal processing; and
- reconciliation and financial reporting.

We evaluated four key risk areas associated with the general ledger module:

1. The risk that chart of accounts changes could be invalid, incomplete, inaccurate or untimely. For example, if the chart of accounts does not remain current (such as inactive accounts remaining active), or if an account is not correct, transactions and related financial information could be incorrect.
2. The risk that if the chart of accounts is not properly structured, the system could produce information that is not meaningful. The chart of accounts dictates how information is to be classified, rolled-up and summarized to produce all financial statements and reports.

3. The risk that journal entries could be invalid, posted more than once, not posted at all, posted to an incorrect period, or posted inaccurately, creating inaccurate information for financial reporting and decision-making.
4. The risk that reconciliation and financial reporting might not be accurate, complete or timely.

What we examined

To evaluate the integrity of the Oracle Financials general ledger module, we identified and tested the control procedures in place for the three main processes of the financial accounting cycle. Our audit also looked at the controls over the data transferred from the Oracle Financials accounts payable sub-ledger, since these transactions have a very significant dollar value.

Controls over budgetary data were outside the scope of our audit. We also did not examine the controls over the transmission of information from sub-systems using the import interface.

Control objectives—chart of accounts data maintenance

We expected to find that:

- additions and changes to the chart of accounts are valid;
- additions and changes to the chart of accounts are complete and accurate; and
- the chart of accounts remains current and relevant (e.g., active accounts remain active).

Control objectives—journal processing

We expected to find that:

- only valid and authorized journal entries are recorded in the general ledger;
- all journal entries are accurate and are posted only once to the general ledger; and
- all journal entries are posted to the correct reporting period.

Control objectives—reconciliation and financial reporting

We expected to find that:

- all financial statement and account reconciliations are complete, accurate and timely; and
- production and distribution of financial reports is timely.

General Ledger Controls

Conclusion

Overall, we found that controls over data entry, processing, validation and management throughout the three main processes of the financial accounting cycle were working effectively. However, we were concerned with the risk of unauthorized changes being made to chart information.

Also of concern was the lack of procedures for monitoring chart data to ensure it is current and relevant for accurate reporting. Management does not seek assurance that the data warehouse (used for creating financial management reports) accurately reflects the data in the Oracle Financials production system. This means that OCG cannot be certain that the data in the data warehouse is accurate and reflects the data in the Oracle Financials production system.

The recommendations concerning the general ledger module controls are listed in Appendix B

Main Findings

Chart of accounts maintenance

A chart of accounts was established as part of the initial set-up of government's set of books. It defines the structure of how accounting information must be collected, categorized, and reported. This structure is made up of seven segments (shown in Exhibit 5): client, responsibility centre, service line, STOB (Standard Object of Expense), project, location, and future. Defining the chart data into independent segments allows flexibility in capturing information relevant to government's current and future financial reporting needs.

Combining these segment values forms an account code that uniquely identifies a general ledger account for recording transactions.

When users record transactions, the segment values are automatically checked to ensure the combination of segments makes sense based on cross-validation rules.

Exhibit 5

The seven segments making up the chart of accounts structure

Segment	1	2	3	4	5	6	7
Name	Client	Responsibility Centre	Service Line	STOB	Project	Location (zero-filled)	Future (zero-filled)
Nature of Information captured	Reporting Entity	Organization unit of the reporting entity that is accountable for the business program or service being delivered	Business program or service being delivered	Classification by account type (asset, liability, equity, revenue, or expense)	A detailed identifier allowing an organization unit to capture project or other detailed information	Allow for future expansion to accommodate possible changes and reporting needs	Allow for future expansion to accommodate possible changes and reporting needs

An account code combination

The chart data that defines the segment values, the rules that link the segment values to form account code combinations, and the hierarchical roll-up of segment values are maintained in tables in the budget and the chart of accounts (BCOA) module that is integrated with the Oracle Financials general ledger.

For the 2004/05 fiscal year, the BCGOV set of books that is maintained in the BCOA has active records of 81,500 segment values, 24,500 rules linking these segment values to form 628,600 account combinations to record transactions, and 16,200 service line roll-up groups to form the chart of accounts.

The records in the chart of accounts are used to classify transactions to the right accounts and generate information for decision-making and financial reporting. If records are not correct, inaccurate transaction reporting and management information could result. Therefore, adequate control procedures are necessary for ensuring these records are valid, complete, accurate and kept current.

General Ledger Controls

Ensuring additions and changes to the chart of accounts are valid

Overall responsibility

There are governing policies and procedures clearly establishing responsibilities and accountabilities over the chart of account structure. The Office of the Comptroller General (OCG) has overall responsibility for the central accounts of government and approval of ministry financial organizational structures. It therefore has the chief role in ensuring that the chart of accounts structure is properly maintained.

Both OCG and ministries share responsibility for maintaining the values of specific segments. As well, ministries are responsible for linking related segment values to form meaningful account code combinations for recording transactions in the general ledger, and OCG is responsible for the roll-up of segment values for financial reporting.

We found that the responsibilities established for chart maintenance were appropriate. However, we are concerned about ongoing maintenance of security access. This poses the risk of unauthorized, invalid changes being made to chart data. Recommendations under our assessment of security administration address this concern.

Segment access rules

Access to chart segments is controlled on an organization basis (an organization is made up of one or several clients). Because financial information is segregated and secured by organization, each ministry can generally use only those assigned values that are within its assigned organization to form account combinations for processing transactions. The Office of the Comptroller General is responsible for maintaining segment values for the client, service line and STOB segments — these three segments are key elements required to produce government's financial statements. Ministries are responsible for the responsibility centre and project segments.

To control access to chart segments, segment access rules appropriately restricts ministry users from setting up client, service line and STOB segments. The rules also define which segments a ministry can use. We found that ministries could use other

ministries' segments—a situation that is not appropriate but which occurs over time as programs change between ministries. Regular monitoring is therefore required.

Although there are clear requirements for OCG to monitor the appropriateness of the rules, we found that procedures have not been established for this purpose, making it difficult for OCG management to help ensure effective operation of the rules and prevent the creation of invalid accounts. We recommend that the segment access rules be periodically reviewed to determine if there are any missed segment value ranges or overlapping ranges that have been created in error.

Incoming segment change requests

Changes to chart segment values are required from time to time to meet operating and reporting needs. Typically, segment values need to be set up when new ministries are created and deactivated when programs end. Chart changes can be initiated by OCG or ministries. Ministry-initiated changes are mostly program specific, relating to service line segment values. Changes initiated by OCG are more government-wide focused, relating to client and STOB segment values.

More than 36,700 chart changes were processed in 2004/05, of which 12% were related to changes made to the three key segments—client, service line and STOB.

A formal chart change request process is in place for those changes that are initiated by ministries. A standard request form must be completed by ministries and submitted to OCG for approval. The request describes the nature of the change and a justification as to why such a change is warranted. We found that ministries monitor this closely to ensure all requested changes are processed promptly by OCG.

Validation of change requests

The Office of the Comptroller General is responsible for carrying out proper assessment and verification procedures to determine the appropriateness of any changes requested, before updating the chart data in Oracle Financials. To assess whether changes are appropriate, OCG first considers whether there are better ways to handle the requests, especially if they would result in a

new segment record having to be added to the chart data. This is a particularly important step to ensure integrity of the chart of accounts. If changes are still deemed necessary, OCG consults the master listing that it maintains separately outside Oracle Financials. This master listing provides a perpetual record of all segment values, with historical information on all past changes. The listing can be used to validate the requested segment value changes. When changes are approved, the OCG master listing and the Oracle Financials chart of accounts are updated.

We found that this is a reasonable process to validate requested segment value changes prior to updating the chart of accounts.

Ensuring additions and changes to the chart of accounts are complete and accurate

Management review of chart of accounts changes

To determine whether changes made to the chart of accounts were input accurately, we examined segment value changes in a four-month period and looked for evidence that OCG validated those change requests. Our testing found that many changes were made without any supporting documentation. This is a concern in view of the differences found in chart information when we compared the chart of accounts and the master listing maintained as a control by OCG. Refer to the "Monitoring the chart of accounts" section for our recommendation.

We believe it is important that a proper audit trail be maintained to support all segment value changes made to the chart of accounts, and for that reason we recommend that procedures be established requiring supporting documentation for all modifications.

Edit and validation checks

Certain settings in Oracle Financials can be used to initiate online edit and validation checks, freeze account structures to prevent future changes, enable dynamic insertion so new accounts can be entered automatically, and enable cross-validation so the validity of new accounts can be checked. We found that all of these settings were being used.

When ministries enter general ledger transactions with new account combinations, the system will check them against the cross-validation rules before allowing them to be used. Proper validation of account combinations depends on how well ministries have defined those rules.

For the ministries reviewed, we found that the cross-validation rules tend to be well defined in the ministries that are organizationally stable and have made few segment value changes over the years. By contrast, the rules are generally poorly maintained in those ministries that have been through several program changes and thus many segment values changes. We also found that validation rules, once defined, were not always reviewed for appropriateness, which means there is a risk of inaccurate entry. We recommend that ministries periodically review the cross-validation rules defined for them to ensure the rules are appropriately set for their needs, allowing proper validation to take place.

Ensuring the chart of accounts remains current and relevant

Monitoring the chart of accounts

As the central agency with overall responsibility for the chart of accounts, OCG must ensure that the integrity of the data is protected, as it is key to accurate reporting. During our review, we found differences in segment values and roll-up information between the chart of accounts and the master listing maintained as a control by OCG.

There are clear requirements setting out the business activities that OCG is required to perform to monitor data integrity of the chart of accounts, as well as the synchronization of data between the chart of accounts and the general ledger. Nevertheless, we found that procedures have not been established for monitoring the chart of accounts to ensure that it is current and relevant. We therefore recommend that OCG formalize and conduct monitoring activities to ensure the integrity of the chart of accounts is maintained.

General Ledger Controls

Journal processing

Journal processing is used for entering, maintaining and reporting on accounting information. Journal entries can be processed directly into the general ledger or imported from a subsystem. Controls should ensure that journal entries posted to the general ledger are accurate, complete and timely. Oracle Financials has many built-in automated features, such as for recurring entries, balancing, edits and validations.

Ensuring only valid and authorized journal entries are recorded in the general ledger

Segregation of incompatible duties

As discussed earlier in the "Security administration controls" section of this report, we are concerned about the ongoing security access maintenance—as this poses the risk of unauthorized journal entries being recorded to the general ledger.

We found that there are effective processes in place to ensure proper authorization and segregation of incompatible duties for journal processing. For example, even though the system allows journals to be entered and posted to the general ledger by the same person, they are manually initiated and authorized by different users thereby achieving the proper segregation of duties. Formal monthly reconciliation processes are also in place to ensure only valid entries are recorded in the general ledger.

Security rules

We also concluded that security rules were effectively controlling and restricting journal entries between ministries. Users are assigned ministry-specific responsibilities and an inter-ministry responsibility. The ministry-specific responsibilities only allow users to enter journals that belong to their ministry. The inter-ministry responsibility allows users to enter journals for other ministries, as security rules do not restrict the use of another ministry's accounts. We understand that to reduce data entry time, some ministries use the inter-ministry responsibility to enter all journals. The security rules designed to prevent incorrect data entry in intra-ministry journals are circumvented by the inappropriate use of the

responsibility for inter-ministry journals. Because this increases the risk of data entry errors, we recommend that management evaluate this risk against the gain in efficiencies.

Automatic entry posting

Certain types of journal batches are automatically posted to the general ledger at night. There is a benefit to ministries of reducing repetitive entries by using this feature, although they need to be aware of the potential for a recurring error if the entry is not properly defined—as this feature is generally used to process recurring or allocation journals.

As this feature was only used by two departments, we recommend that ministries review their needs and requirements, and determine if they could benefit from the use of recurring or allocation journals to allow for more efficient and effective journal processing.

Ensuring all journal entries are accurate and are posted only once to the general ledger

Batch naming conventions

Because users are able to access and post journals that belong to other ministries, it is important that clear and consistent journal batch naming conventions be established and used to minimize the risk of posting another ministry's journals. A batch naming convention unique to each ministry allows transactions to be identified, tracked and reviewed. The minimum naming requirement is that each batch name begins with a two-letter ministry identifier, followed by a two-digit fiscal year. For example, a journal batch name "FI05" refers to a batch created for Ministry of Finance for the fiscal year ending March 31, 2005.

We found that journal batch naming conventions are generally not being followed across government. To ensure that all journal batches are clearly distinguished, we recommend that ministries adhere to established batch naming conventions when creating journal batches in the Oracle Financials general ledger.

Edit and validation checks

One of the main ways of ensuring that journal entries are accurate and balanced is by configuring edit and validation checks in Oracle Financials. The system edits and validates the entry of data in a number of ways: some fields are mandatory to complete; some fields validate the value entered against a corresponding table; some fields have a list of values to choose from; and some fields are automatically filled in with default values. We found all of these checks being used, and noted that controls to protect posted journal entries from modification are also in effect.

When unbalanced journal entries are entered into the Oracle Financials general ledger, the system will either reject the transactions or force them to balance by posting the differences to a suspense account. We verified that the option for suspense account posting is not enabled, which means out-of-balance postings are prevented in the government's general ledger.

All manual journal entries should be batched for processing. A batch may consist of many journal entries. To ensure that data entry is accurate, the Oracle Financials general ledger provides a "control total" feature that checks the totals for the journal batch as well as the individual journal entries in a batch. The use of the control total feature when entering journal entries is not mandatory; and even when used, the system will not prevent posting if batches do not match the control totals. However, warning messages will be displayed to warn users of the difference. The ministries we reviewed were using this feature appropriately.

To identify a journal entry as a duplicate, Oracle Financials checks the combination of journal name, batch name and date. The system verifies that the combination of these three fields is unique before accepting the entry. We found that the design of this control feature does not prevent a journal entry from being posted twice. For example, a journal entry that is entered into the system for a second time under a different batch name would not be identified as a duplication. Reliance must be placed on control processes set up in ministries to ensure journals are not processed twice. For the ministries we reviewed, we found that proper control processes were not always in place. We therefore recommend that ministries review their processes to ensure they have proper procedures for preventing duplicate journal entries.

Ensuring all journal entries are posted to the correct reporting period

Oracle Financials requires an accounting calendar, outlining the accounting year and reporting periods. We verified that the system has 12 periods, plus adjustment periods, in its accounting year. We also verified that a journal entry could not be created for a previous period and, although it could be created for a future period, it could not be posted.

In closing off each accounting period for reporting, a certain sequence must be followed in Oracle Financials. The period is first closed for each subsidiary ledger, before the general ledger closes. Periods can be re-opened, but only when it is necessary to do so and then only under restricted circumstances. Normally only one accounting period is open, except at year-end where two periods are open to allow transactions to be posted for the old fiscal year and the new fiscal year.

We found that formal monthly reconciliation processes are in place to ensure all entries are posted to the general ledger and to the correct accounting period.

Reconciliation and financial reporting

Both reconciliation and month-end financial reporting procedures have been established in ministries and the OCG.

Financial reports produced by OCG are based on data from the Corporate Accounting System Open Data Exchange (CODE) data warehouse. Data is transferred nightly from Oracle Financials to the CODE data warehouse, so it is important that the information in CODE be an accurate and complete reflection of the information stored in Oracle Financials.

Our audit focus was on the Oracle Financials application. We did not examine the controls related to the CODE data warehouse. We expected management, as part of its financial reporting processes, to have procedures in place to ensure that the data in CODE is a complete, accurate and timely reflection of the data in the Oracle Financials production system.

Ensuring all financial statement and account reconciliations are complete, accurate and timely

Reconciliation with data warehouse

Our review and walkthrough of the OCG financial reporting processes confirmed that a formal monthly process is in place to generate financial reports from CODE at each period close, and that financial reports generated were reconciled to general ledger account balances in CODE. As well, OCG does perform some review of the Oracle Financials data at each period-end to ensure completeness of data captured in CODE.

One deficiency we noted, however, was that OCG management did not have an established procedure that compares the financial data recorded in the Oracle Financials with that in the data warehouse to assure them of the integrity of the CODE data used for financial reporting. This means that OCG cannot be certain that the data in CODE is accurate and reflects the data in the Oracle Financials production system. We recommend that a reconciliation procedure be established to provide OCG management with the necessary assurance on this issue.

Reconciliation with sub-ledgers

Ministries are responsible for the complete and accurate recording of transactions in Oracle Financials and for ensuring Oracle Financials reflects the correct current year-to-date balances. Ministries are also responsible for reconciling sub-ledgers to the general ledger. Clear procedural documentation sets out the month-end closing and reporting requirements for ministries.

We found that not all ministries were reconciling the Oracle Financials accounts payable sub-ledger to the general ledger. We were satisfied that all validated transactions in the accounts payable sub-ledger were properly transferred and posted to the general ledger. However, we noted that a small number of transactions existed in the sub-ledger for a period of two years that were not validated for posting to the general ledger. We think that if ministries had performed the reconciliation, these outstanding transactions would have been identified and corrected on a

timely basis. Therefore, we recommend that the requirement and responsibility for reconciliations be clearly communicated to the ministries.

Greater use by ministries of a reconciliation schedule, which also includes the reconciliation of accounts payable sub-ledger to the general ledger, would help them better monitor and oversee the month-end reconciliation process to ensure all reconciliations are being performed. We recommend that reconciliation schedules be used.

Ensuring production and distribution of financial reports is timely

Month-end and fiscal year-end reporting requirements are clearly specified, as are the procedures outlining the required activities and timelines.

Responsibility for the financial reporting function is OCG's, which generates monthly financial reports for internal reporting and publishes quarterly financial operating results. Government's financial statements for the fiscal year are audited and published annually in the Public Accounts. We were satisfied with the process that OCG management has in place to ensure the timely generation of financial reports.

Supplier Maintenance Controls

Controls over the supplier master data are necessary to ensure that supplier information is kept current and that changes to the information are valid, complete, accurate and timely.

The supplier master data is a central component within Oracle Financials that impacts transaction processing within the purchasing and accounts payable modules. It contains information about all the individuals, businesses, and organizations from whom the government purchases goods and services and to whom it pays grants.

Suppliers are classified into three types: general supplier, block supplier, and employee supplier. The general supplier category is typically used for processing purchase orders for goods and services. The block supplier category is used for recording payments (often one-time payments) that are made to multiple payees—without each payee having to be set-up as a supplier. For example, block suppliers are used for paying scholarships to students through universities and colleges. The employee supplier category is used primarily for reimbursing employees for their business travel expense claims.

Travel expense claims are processed through the CAS Oracle iExpense Self-Service module. Because that module was outside the scope of our review, we did not examine the integrity of the employee supplier data. We did, however, run tests on the supplier data that included these suppliers.

At the time of our audit, the supplier table contained over 275,000 records (see Exhibit 6). Each record represents an individual supplier and contains key information such as the supplier's name, address, bank details, payment method and, when required, bank account information for generating electronic payments.

Exhibit 6

Number of records by supplier types, as at August 2004

	Active	Inactive	Total	%
General	224,300	6,800	231,100	84
Block	400	100	500	–
Employee	30,000	13,800	43,800	16
Total	254,700	20,700	275,400	100

Source: Compiled from the Oracle Financials supplier table

We evaluated four key risk areas associated with supplier maintenance:

1. The risk that goods and services could be acquired from unapproved or obsolete suppliers.
2. The risk that payments could be sent to incorrect addresses.
3. The risk that payments could be made to wrong bank accounts.
4. The risk that unauthorized payments could be made.

It is therefore important for all of these risks that access to this information be appropriately restricted and that only valid suppliers with valid information be maintained in the system.

What we examined

We tested the control procedures in place to evaluate the integrity of supplier information and to determine their effectiveness in reducing the identified risks.

Control objectives for maintenance of supplier information

We expected to find that:

- access to create and change supplier information is appropriately restricted to authorized individuals;
- configurable controls are designed into the process to maintain the integrity of supplier information;
- additions and changes to the supplier information are valid, complete, accurate and timely;
- supplier information remains current and relevant;
- additions and changes to the supplier banking information are valid, complete, accurate and timely; and
- supplier bank information remains current and relevant.

We checked:

- who has access to what supplier information and at what level, and whether those users are required to have that access for business purposes;
- what built-in system controls are being used;
- how suppliers are initially set up to do business with government; and
- what review and monitoring management does to ensure additions and changes to supplier information are correct, valid and complete.

Conclusion

We were not satisfied that management has adequate controls in place to manage some risks, such as the redirection of supplier payments. Controls need to be strengthened to ensure the initial accuracy and validity of supplier information and to address the ongoing challenge of ensuring the information remains current.

- One area of concern is how supplier names and addresses are entered. Because compliance with the established naming convention for supplier names is not consistently used, there are many of what appear to be duplicate suppliers (similar supplier names with the same address). Not only does this hinder the search capability on supplier names, but it indicates that verification checks are not always catching or preventing irregularities.
- "Generic" suppliers (those set up so that one supplier record serves multiple suppliers—the name and supplier number are the same and only the address varies for each supplier) also pose risks. If correct addresses are not selected during invoice processing, cheques could inadvertently be sent to the wrong suppliers and potentially even be cashed by the recipients.
- Total amounts paid to each supplier who received more than $25,000 for the fiscal year are reported in the a supplementary schedule to government's financial statements. However, suppliers paid through the block supplier category are not reported. We are concerned that some of these payments should be included and therefore

there is a risk of non-compliance with government's reporting requirements.

- Weaknesses in the way bank account change requests are handled are also putting the validity, accuracy and completeness of supplier information at risk. One problem is the lack of verification by ministries to ensure that suppliers requesting the changes are in fact legitimate. Unless individuals or organizations providing the bank account information are verified to have the authority to do so, there is a risk that payments could be redirected from existing suppliers' bank accounts to fraudulent ones.
- Appropriate monitoring is put in place that checks any new or changed bank accounts against the original deposit application forms to provide assurance that no unauthorized or inappropriate changes to linked bank accounts have occurred. However, there is no similar monitoring to ensure that all supplier linkages to a bank account are valid.
- Suppliers are required to submit direct deposit application forms to establish or change bank accounts. Copies of these forms, which contain confidential information, are retained by each of the user groups involved in bank maintenance. These forms are often kept in areas accessible by many people, potentially compromising the security of suppliers' information.

The recommendations concerning supplier maintenance controls are listed in Appendix B.

Main findings

Ensuring access to create and change supplier information is appropriately restricted to authorized individuals

There are established roles and responsibilities for each user group involved in maintaining supplier information. User guides provide clear step-by-step guidance on maintenance procedures.

- Ministry supplier maintenance staff are responsible for inputting, and submitting changes, based on information received from suppliers. Corporate Accounting Services staff are responsible for validating and updating the changes input by ministries.

- Ministry staff are responsible for reviewing the suppliers' requests for electronic payments to ensure they are complete. Provincial Treasury staff are responsible for examining and entering bank account information based on these requests, while Corporate Accounting Services staff are responsible for linking the bank accounts entered by the Provincial Treasury staff to individual suppliers.
- The Office of the Comptroller General staff are responsible for approving the set-up of block suppliers and maintaining stop payments to suppliers.

We found that the activities assigned to responsibilities established for supplier maintenance are appropriate and incompatible functions are segregated (for example, entering suppliers' banking information and linking of the information to suppliers are segregated).

However, the lack of an effective ongoing security access maintenance process concerned us. This could result in unauthorized, invalid changes being made to supplier data. Our recommendations related to this issue are included in the "Security administration controls" section of this report.

Ensuring configurable controls are designed into the process to maintain the integrity of supplier information

Several system settings—for example, enabling the automatic assignment of numeric supplier numbers—can be set in Oracle Financials to control the entry of supplier information. We tested a selection of these configurable controls in CAS and found them to generally be working as intended.

One exception was the control over address fields. We found some suppliers with missing address information. However, because these suppliers were created before the implementation of Oracle Financials, we believe these cases might be the result of the conversion from the previous accounting system to Oracle Financials, and not a systematic problem in Oracle Financials. We recommend updating the suppliers with missing address information.

Ensuring additions and changes to the supplier information are valid, complete, accurate and timely

Additions and changes to supplier information

Changes to supplier information are required from time to time to meet business operating needs. It is important that the supplier information be maintained accurately to ensure that payments are made to the correct supplier and cheques are mailed to the correct address.

Requests describing changes to supplier information—adding new suppliers, modifying information for existing suppliers or inactivating existing ones—are forwarded through electronic mail to ministry supplier maintenance staff. We found that these staff do not always request or use the originating documents to confirm the accuracy and validity of the information in the change requests. This creates a risk that supplier information may not be correctly entered. We recommend that procedures be established requiring copies of supplier invoices or other documentation supporting the requested changes be forwarded to supplier maintenance staff.

Upon receiving a request for changes, ministry supplier maintenance staff conduct a search using the supplier name to identify whether that name already exists. The effectiveness of ministry duplicate supplier searches depends on how well the supplier naming conventions are being followed.

Because it is not uncommon to have suppliers with the same name, a naming convention has been established. However, lack of diligence in following the convention (and in entering address data) not only makes a search for duplicate suppliers difficult, it also suggests that a stronger verification check is needed to ensure that the same suppliers do not already exist (see our findings below under "Compliance with name and address standards"). We recommend that verification procedures be strengthened to include a search on supplier addresses.

For ministry-initiated changes, we found that responsibilities are properly segregated to prevent staff from having the ability to enter both the supplier change information and update the supplier data. However, for changes that come directly to Corporate Accounting Services from suppliers, the two activities (entering and updating) are usually performed by the same staff. In view of the fact that CAS

support staff generally have potential for unlimited access to the system, this is one of the high risk areas that requires monitoring. (Refer to our assessment under "Monitoring high-risk activities" in the security administration section of this report.)

Compliance with name and address standards

Supplier names entered using a consistent naming convention assist users in identifying the correct suppliers for payment, and minimizes the risk of creating duplicate supplier records. Addresses that are complete minimize the risk of mailed cheque payments going astray. The complete address also assists in identifying the correct suppliers for payment, especially when there are a few suppliers with similar names.

The system does not allow suppliers to have exactly the same name. A standard naming convention has therefore been established to allow adding appropriate details (such as a full middle name, a second initial or an asterisk) to each new supplier name to make it unique. The standard for system addresses is based on the format specified in Canada Post guidelines. All components of an address—including the postal code—must be present, correct and match the information on Canada Post's address database. Any mailings that fail the match are returned to Corporate Accounting Services for correction. This external verification process ensures accuracy of the address format.

In our review we found many instances where the supplier names did not adhere to the established naming convention and recommend that they be corrected. Although many were records transferred from the previous accounting system, we believe there is still a problem with non-compliance. We therefore recommend that Corporate Accounting Services reinforce with ministry staff the importance of following the standard naming and addressing conventions when entering new supplier information, and also recommend that procedures be established for periodically reviewing the supplier data format for consistency and compliance.

Supplier Maintenance Controls

Ensuring supplier information remains current and relevant

Corporate Accounting Services has overall responsibility for ensuring that the information maintained in the supplier table is current and relevant. To evaluate the reliability and integrity of the supplier information, we looked at the existence of possible duplicate suppliers, inactive suppliers, multiple suppliers within a supplier record (the "generic suppliers"), and the management of block suppliers. These situations could lessen the integrity of the supplier information and increase the risk of payments being made to incorrect suppliers.

As of August 2004, the supplier tables contained about 224,000 active general supplier records. Of these, we found that more than 92,000, about 41%, had the same address as another supplier. We recognize there are many circumstances where it is reasonable for suppliers to share the same address. For example, when the suppliers are business partners; business entities and their owners; doctors sharing a clinic; law firms and their partners; or pharmacies and associated chain stores.

However, the large number of addresses with more than one supplier recorded at the same address may indicate that: suppliers are being recorded more than once, suppliers have moved but address sites remain active, and suppliers have ceased operations but remain active in the supplier listing. We have addressed these situations below.

Information relevancy through management monitoring

While there are clear procedures to review, validate and approve supplier change information, procedures have not been established to periodically monitor and review the supplier information to ensure it remains current and relevant. This increases the risk of incorrect suppliers being selected for payment.

Corporate Accounting Services completed a one-time purging process on supplier data in September 2005. The purge process successfully removed about 93,800 suppliers that had not been used since 2001 and 5.2 million related addresses from production. This was a positive step towards reducing the risk of paying incorrect suppliers. Nonetheless, adequate ongoing review

and monitoring procedures are essential to ensure the supplier information remains current and relevant. We recommend that these review and monitoring procedures be put in place.

Monitoring general suppliers for duplicates

To evaluate whether duplicate suppliers exist, we focused our review on examining suppliers with similar names. We estimated that about 5,700 duplicate suppliers existed in the data as of August 2004—or 2.5% of all active general suppliers.

Several weaknesses with the supplier maintenance process contributed to this duplication problem:

1. Although a standard naming convention had been established, including using full names for entering suppliers, this was not always adhered to. Not only were partial names of suppliers being used, we also found non-specific names (for example, "Computer Centre," "Out of School Care"). Because supplier names were not entered consistently, the effectiveness of the system's search capability on supplier names is weakened.

2. The inconsistency in supplier naming practices led us to believe that supplier names were sometimes being entered without adequate verification against supporting documents and without checking for compliance with the naming convention.

3. The current search capability to identify whether suppliers, or suppliers with the same name, already exist, is restricted to a search only on the supplier name field. The effectiveness of the search depends not only on the consistent use of the naming convention, but also on the search criteria used. In our view, a search on addresses as well could help to identify possible duplicates or other irregularities.

To maintain the integrity of supplier information, we recommend that Corporate Accounting Services periodically review the supplier data for duplicate suppliers and deactivate any that are found.

Supplier Maintenance Controls

Monitoring employee suppliers for duplicates

When the prior accounting system was replaced with Oracle Financials, all existing suppliers, including employees, were added to the Oracle supplier tables as general suppliers.

In September 2002, the CAS Oracle iExpense Self-Service module was implemented, allowing government employees to process travel-related expenses. All employees were set up as employee suppliers in the supplier data. This resulted in two supplier records being created for the same employee—once as a general supplier and again as an employee supplier. In most cases the general supplier record is no longer needed and Corporate Accounting Services has been deactivating these over time. In our examination of the supplier table as of August 2004, we found that about 2,200 employees still had both types of records. This issue is addressed in our recommendation above.

Monitoring inactive suppliers

As suppliers typically do not report on their status (such as whether they have ceased operations, changed names or moved), Corporate Accounting Services cannot ensure that all supplier records are current and up-to-date. This adds complexity to the supplier maintenance function, and underscores the importance of monitoring. Enhancing the current supplier search capability to include an address search would not only help identify duplicate records, but would also help identify suppliers with the same address (and therefore entries that may be invalid or require updating).

We found that no formal monitoring activities were being done to routinely identify duplicate suppliers or to deactivate suppliers. The status of suppliers is changed only when notifications are received that they have ceased operations, changed names, or when they have been identified as duplicates. Once deactivated, transactions can no longer be processed against these suppliers.

Most businesses in the supplier table are also registered with the provincial Corporate Registry. These entities are assigned individual business registration numbers that serve as unique identifiers. This makes online searches for particular businesses relatively simple. We believe that matching to the Corporate Registry could be helpful in confirming supplier status in the CAS supplier table.

We recommend that Corporate Accounting Services consider implementing a data-matching process comparing information on the supplier table with the provincial Corporate Registry so that supplier records can be updated to reflect current statuses for business suppliers. To facilitate this data-matching process, we recommend procedures be established to require the collection of the business registration numbers for all new business suppliers and, when practical, also for existing business suppliers.

Monitoring multiple suppliers within one supplier record

Each supplier is normally assigned a unique supplier number as an identifier. This allows government to track and report the total amount paid to each supplier. Each supplier number (except for the block supplier type) is associated with only one supplier to form a supplier record in the supplier table. Supplier records are linked to their address sites in the site table. Suppliers may also have more than one address.

Some supplier records, however—so-called "generic" suppliers—are set up in such a way that individual records represent multiple suppliers. Suppliers with the same last name and first initial are entered under a single supplier record, sharing one supplier number. The supplier record is linked to several address records which are the addresses for each individual supplier. Even though these are individual suppliers, since they share the same supplier number, they cannot be separately identified.

Generic supplier records were first created in government's old financial system, which had a limit on the number of supplier records that could be created. The use of generic suppliers provided a way of adding more suppliers without increasing the number of supplier records. We understand that Oracle Financials does not have such a limitation, so there is no longer a need to create generic suppliers.

There is no easy way to identify generic supplier records because there is no unique identifier that flags these records. Corporate Accounting Services was unable to tell how many of them were in the supplier table.

The existence of generic suppliers concerns us for several reasons:

1. Generic suppliers, like other suppliers, can receive payments. The only way to uniquely identify generic suppliers is by addresses. If the incorrect address is selected when invoices are processed, cheques could be sent to the wrong supplier, and could even be cashed by the recipient (who has the same name as the payee).
2. When electronic banking is requested by one of the suppliers of a generic supplier, there is a risk that bank account details could be incorrectly linked to the wrong address record. Payments could therefore be deposited erroneously to bank accounts that belong to other suppliers. Corporate Accounting Services has already identified this risk and does not allow bank accounts for electronic payments to be linked to generic supplier records. However, given that generic suppliers are not easily identifiable, we questioned how well the practice was being complied with and monitored.
3. Since generic suppliers are often only listed by last name and first initial, name searches may fail to find another record containing a slightly different form of the name. This could result in supplier records being added for the same suppliers.
4. There is also a risk of non-compliance with financial reporting requirements. The supplier number is the key that allows government to report total amounts paid to each supplier. Because all suppliers within a generic supplier record share the same supplier number and payment history, payments received by individual suppliers of a generic supplier are not identifiable or reportable.

We recommend that Corporate Accounting Services establish formal policies restricting further set-up of generic suppliers and formalize a plan to use, manage and update generic supplier records.

Managing the use of block suppliers

In 2004/05, about $200 million in expenses were processed through CAS to over 55,000 payees via about 120 block suppliers. The use of block suppliers greatly reduces the number of individual suppliers that would otherwise need to be set up on the system

(such as for individual suppliers receiving small dollar, often one-time, payments—for example, scholarships paid to students directly or through post-secondary institutions).

There is documentation outlining some high-level guidance to ministries as to when block suppliers could be used for processing payments. However, we believe that ministries require more clarity in their decisions for using block suppliers and therefore recommend that clear policies and guidelines be established for using block suppliers in processing payments. OCG should also establish clear criteria for monitoring and compliance activities.

There are several risk exposures when using block suppliers for payment:

1. Processing block supplier invoices requires name and address overrides to be used (the actual payees' names and addresses). This introduces a risk that payments may be redirected to unauthorized payees.
2. Total amounts paid to each supplier who received more than $25,000 for the fiscal year are reported in a supplementary schedule to the government's financial statements. Since we found block supplier payees that had been paid more than $25,000 during the fiscal year 2004/2005, we are concerned that some of these payments should have been reported under government's reporting requirements.
3. It is not possible to apply stop payments against block supplier payees since they do not exist in the supplier table. As a result, there is a risk that payments may be made to block supplier payees that cannot be stopped or diverted.
4. Block suppliers are often used for payments for specific programs where reporting actual suppliers may have privacy impacts. It was beyond the scope of this audit to determine whether there really was adequate privacy protection over data stored in Oracle Financials. However, for some payment types—including victim assistance and provider payments, jurors payments, and witness payments—the suppliers' identities, when disclosed, could have privacy implications. We recommend that appropriate procedures be established to ensure proper processing of payments with due regard to confidentiality of data.

Supplier Maintenance Controls

Ensuring additions and changes to the supplier banking information are valid, complete, accurate and timely

Suppliers are paid by hard copy cheque or direct deposit. The method of payment is recorded on each supplier record. If payments are by cheque, addresses from the supplier table are used for the mailing addresses. If suppliers request electronic payment through direct deposit, the bank account information must be recorded in the supplier record. It is therefore important that the information directing the payments be accurate and up-to-date.

The responsibility to maintain supplier bank account information is shared among ministries, Provincial Treasury and Corporate Accounting Services. Ministry staff are responsible for reviewing the completed electronic payment deposit request forms originated by suppliers for completeness and accuracy. Provincial Treasury staff are responsible for reviewing, validating and entering the bank account information based on suppliers' requests for electronic payments. And Corporate Accounting Services staff are responsible for linking the bank accounts entered to suppliers.

By means of assigned user roles—between Provincial Treasury and Corporate Accounting Services staff—bank account maintenance functions are properly restricted, and responsibilities are properly segregated. Segregation of incompatible duties is a strong control procedure for ensuring validity of banking records maintained in the supplier table. We found that access to update the bank account table is restricted to the Provincial Treasury staff, while access to update suppliers and supplier site tables is restricted to Corporate Accounting Services staff.

A formal supplier bank account change request process is in place to set up electronic payments, change accounts, or discontinue electronic payment deposits.

We found that the roles and responsibilities that ministries play in reviewing the bank account change information is unclear. We are concerned about the extent of verification work performed in ministries to ensure requests are complete and changes are legitimate and recommend that policies and procedures be established to address this concern.

We also recommend that there be verification of requested changes by calling suppliers using contact information retrieved either from existing supplier records or from sources other than the contact information on the forms submitted by suppliers.

Several other weaknesses were identified in the way bank account changes are handled, creating a risk that payments could be redirected from existing suppliers' bank accounts to fraudulent ones. We believe this is due to a lack of awareness of potential threats and risks associated with banking activities and recommend that OCG strengthen this awareness.

Ensuring supplier bank information remains current and relevant

Activities affecting supplier banking information must be adequately monitored to ensure the information remains current and relevant. Without adequate monitoring, there is a risk of payments being made to invalid suppliers.

By means of proper segregation of duties, Provincial Treasury staff are responsible for adding or changing bank account information for suppliers, while Corporate Accounting Services staff are responsible for linking bank account information entered to correct suppliers. Appropriate monitoring is put in place that checks any new or changed bank accounts against original deposit application forms to provide assurance that no unauthorized or inappropriate changes to linked bank accounts have occurred.

However, there is no similar monitoring to ensure that all supplier linkages to a bank account are valid. When links from suppliers to bank accounts are made, payments are automatically directed to the linked bank accounts. If the links were incorrect due to error or fraud, the payments would be deposited to incorrect bank accounts. Linking bank accounts is a high-risk activity and we recommend that it be actively monitored, in particular, given that some CAS support staff have the potential to gain unlimited access to the system.

As noted earlier, suppliers may have more than one supplier site. A business decision was made that only one active bank account may be linked to a supplier. The system, however, does not enforce this and we found instances where suppliers had a different bank account number for each of their address sites. This means that

payments to each address site would be directed to a different account. We recommend that procedures be established to address this concern.

In some situations, bank accounts can also be shared by more than one supplier. An account can be flagged and set to allow assignment of the same account to multiple suppliers. This prevents the risk that the same bank account be inadvertently set up for a second time for another supplier. We found a deficiency where disabling the multiple supplier assignment flag does not prevent the bank account from being assigned to more than one supplier. We recommend that periodic reviews be carried out to ensure that bank accounts that have not been flagged are not assigned to more than one supplier.

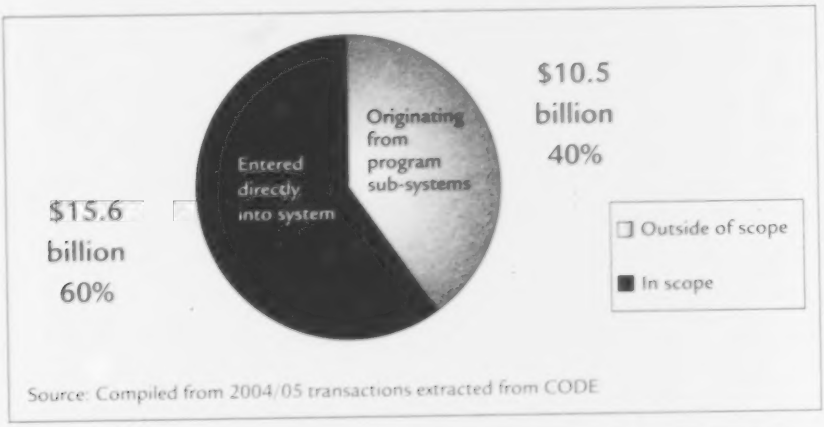
Our final concern related to the security of the completed change request forms. The personal and confidential information detailing the suppliers' bank accounts is sensitive and could have privacy implications. We noticed, however, that copies of these completed forms are retained by each of the user groups involved in bank maintenance (ministries, Provincial Treasury and Corporate Accounting Services)—and were kept in areas of these offices that are accessible by many people. We are concerned about the security access to these forms and recommend that management address this issue.

Controls over purchasing and accounts payable are necessary to ensure (1) that government pays the correct amounts to the correct suppliers for authorized – and delivered – goods and services only and (2) that all outstanding orders and payments are accurately and completely recorded.

During fiscal 2004/2005, over 4 million expenditure-related transactions were processed through CAS, resulting in $26 billion being recorded as expenses in government's financial statements. These transactions represent the costs to deliver many government programs, and are categorized as salaries and benefits, operating costs, government transfers, interest expense and other expenses. They were either entered directly into the purchasing and accounts payable modules in Oracle Financials, or processed in a sub-system and entered through the system interface. As shown in Exhibit 7, our audit only looked at controls over those transactions entered directly into Oracle Financials, which represents about 60% of the total expenses.

Exhibit 7

Expense transactions processed through the purchasing and accounts payable modules



Source: Compiled from 2004/05 transactions extracted from CODE

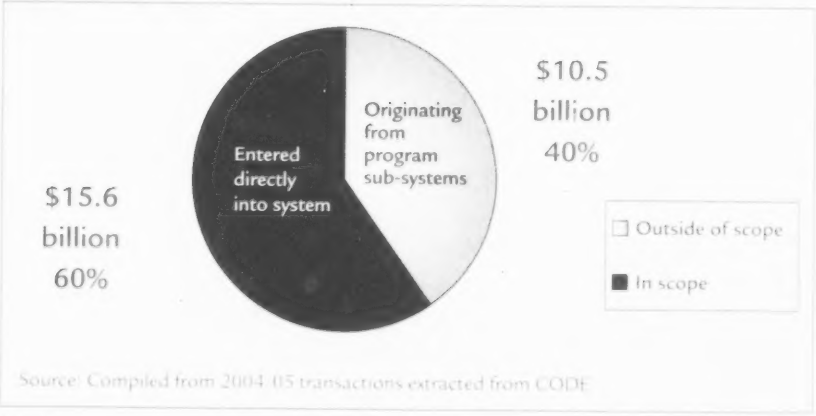
Note:
The expense transactions within the scope of our audit are those that are processed through the purchasing and accounts payable modules in Oracle Financials. These transactions recorded expenses that can be categorized as – salaries and benefits $0.3 billion, operating costs $2.0 billion, government transfers $11.6 billion, interest expense $1.6 billion, and other expenses $0.1 billion – totalling $15.6 billion.
The expense transactions outside the scope of our audit originated from program sub-systems and are transferred to Oracle Financials through the interface system. These transactions recorded expenses that can be categorized as – salaries and benefits $1.9 billion, operating costs $1.1 billion, government transfers $9.7 billion, interest expense $0.7 billion, other expenses $1.3 billion, and recoveries $(4.2) billion – totalling $10.5 billion.

Controls over purchasing and accounts payable are necessary to ensure (1) that government pays the correct amounts to the correct suppliers for authorized – and delivered – goods and services only and (2) that all outstanding orders and payments are accurately and completely recorded.

During fiscal 2004/2005, over 4 million expenditure-related transactions were processed through CAS, resulting in $26 billion being recorded as expenses in government's financial statements. These transactions represent the costs to deliver many government programs, and are categorized as salaries and benefits, operating costs, government transfers, interest expense and other expenses. They were either entered directly into the purchasing and accounts payable modules in Oracle Financials, or processed in a sub-system and entered through the system interface. As shown in Exhibit 7, our audit only looked at controls over those transactions entered directly into Oracle Financials, which represents about 60% of the total expenses.

Exhibit 7

Expense transactions processed through the purchasing and accounts payable modules



Source: Compiled from 2004/05 transactions extracted from CODE

Note:

The expense transactions within the scope of our audit are those that are processed through the purchasing and accounts payable modules in Oracle Financials. These transactions recorded expenses that can be categorized as – salaries and benefits $0.3 billion, operating costs $2.0 billion, government transfers $11.6 billion, interest expense $1.6 billion, and other expenses $0.1 billion – totalling $15.6 billion.

The expense transactions outside the scope of our audit originated from program sub-systems and are transferred to Oracle Financials through the interface system. These transactions recorded expenses that can be categorized as – salaries and benefits $1.9 billion, operating costs $1.1 billion, government transfers $9.7 billion, interest expense $0.7 billion, other expenses $1.3 billion, and recoveries $(4.2) billion – totalling $10.5 billion.

Purchasing and Accounts Payable Controls

In the fall of 2004, government introduced the Oracle iProcurement system to integrate the business processes in purchasing and accounts payable functions. Oracle iProcurement allows the purchase of goods and services through the use of online requisitions and approvals. The process involves online approvals of requisitions or purchase orders by authorized staff and online receipt of goods and services to automatically generate supplier payments and complete the purchase process.

The information used to direct the payments to supplier addresses or bank accounts comes from the supplier master table, which is shared by all ministries. The examination of the controls and business processes over the maintenance of supplier information are discussed in the supplier maintenance section of this report.

The purchasing and accounts payable modules are tightly integrated. Both share supplier data and often involve the same transactions. Purchasing validates payment obligations through a process that matches invoice details to purchase orders and goods or services received. Matched invoices do not require further expense authority approval since approvals were already received at the requisition or purchase order level. In some cases, such as purchases using corporate credit cards, invoices are entered directly into accounts payable. These "direct" invoices require online invoice approvals from appropriate expense authorities before payments can be generated. (Refer to the following side bar for information on expense authorities.)

Purchasing and Accounts Payable Controls

A new control framework

Accountability and responsibility for spending public money is placed on ministers and deputy ministers. In order for them to carry out their responsibilities, ministers and deputy ministers delegate their financial signing authority to ministry officials, to excise responsibilities on their behalf. Historically, responsibility to authorize expenditures was delegated to one official who authorized the spending (spending authority) and another who authorized the payment (payment authority). They were required to review expenditures and verify compliance with financial policies before payment was made.

On April 1, 2004, amendments to the ***Financial Administration Act*** brought about some significant changes to the expenditure control framework. These amendments shifted the backend payment authorization control (when an expenditure is reviewed for financial compliance prior to a payment being made) to a more upfront control (when an expenditure is initiated).

What this means: The requirement for a payment authority to approve expenditures before payment has been eliminated. The responsibility to authorize expenditures for both spending and payment has been shifted to just one official, an expense authority – a new role that was created as a result of the change in the control framework. The framework has changed from detailed compliance and pre-audit checks before payment to post-payment reviews by the Payment Review Office (PRO) to verify payments.

Under the new expenditure control framework, the expense authority is responsible for authorizing expenditures. That individual is accountable for all purchases he or she approves. When approving transactions, expense authorities have the responsibility to ensure that an expense is properly charged against a budget, does not exceed the available budget, and complies with all relevant statutes and policies. To provide for proper control and integrity of the process, a person other than the expense authority (who approves the purchase) must receive the goods and services. As well, the PRO is responsible for reviewing payments after the fact to verify compliance with financial polices and legislation.

The PRO, established in November 2001 as part of the Office of the Comptroller General, acts as a financial control by providing a "threat of detection." In this way, it ensures compliance with policy and legislation and thereby reduces financial loss to the government. The PRO uses a risk-based approach to test payment transactions for compliance with financial policies and legislation. Given the changes in the control framework that resulted from the introduction of iProcurement, the extent of testing performed by the PRO was increased, starting in January 2004.

Also, as part of the new control framework, there is a reporting obligation for public service employees to report to the Comptroller General if they consider an expenditure authorization or payment to be inappropriate or not compliant with legislation.

We evaluated four key risk areas associated with the purchasing and accounts payable modules:

1. The risk that the entry of, or changes to, purchase orders could be invalid, incomplete, inaccurate or untimely, leading to financial loss.
2. The risk that amounts posted to accounts payable might not represent goods or services received, resulting in unauthorized payments being made.
3. The risk that accounts payable amounts might not be recorded completely, accurately or promptly.
4. The risk that unauthorized payments could be made to fictitious suppliers.

Purchasing and Accounts Payable Controls

What we examined

In examining the controls related to the purchasing and accounts payable modules, we focused on those controls that would address these four key risk areas. Our work included assessing security management and the controls set up to ensure proper access to the modules and proper authority to approve transactions.

Control objectives for security management and authority to approve purchase and accounts payable transactions

We expected to find that:

- access to create, change or cancel purchase requisitions, purchase orders and invoices is appropriately restricted to authorized individuals;
- Oracle Financials approval levels are secured and configured in conformity with established business requirements;
- payments are only made for authorized purchases and for goods and services received; and
- key financial reports are reviewed and monitored to ensure validity, completeness and accuracy of recorded transactions.

Specifically, we checked:

- who has access to create, change or cancel purchase requisitions, purchase orders and invoices, and whether accesses were appropriate based on business needs;
- how approval authorities are set up; and
- whether system controls and business processes properly support the intended approval process.

Our examination of the purchasing and accounts payable modules did not include expense transactions that originated from sub-systems and were transferred to Oracle Financials through the interface system. Also, our scope did not include reviewing the actual production of cheque and electronic payments, as these payment details are exported from Oracle Financials to a separate system responsible for cheque production and sending electronic payment information to banks.

Conclusion

We found that access controls for the purchasing and accounts payable modules were for the most part appropriate. However, we did identify several areas of concern where we believe controls could be improved.

The control environment involves the use of system-based controls together with manual business controls, requiring a balance between the two to mitigate the risk of fraud and error. Because system-based controls are not strong enough on their own to prevent or detect errors or fraud, reliance is also placed on business controls that allow the processing results to be reviewed for completeness and accuracy. The review of financial management reports is therefore an important control for monitoring expenditures. We found that this was being done, but the effectiveness of the review could be improved.

Oracle responsibilities that allow users to only perform certain activities were not always restricted to appropriate individuals. We found that incompatible responsibilities were assigned to some expense authorities giving them excessive access privileges to the system. The process to review expense authority access, to ensure it remains appropriate to their roles, needs to be improved.

Under the new expenditure control framework associated with iProcurement, the expense authority has an important role to play. We concluded that government has set clear policies and procedures establishing accountabilities and responsibilities for the control and management of government expenses. However, we had some concerns with the way the approval process is handled:

- The maintenance of expense authority approval levels and their assignment is centrally administered in ministries by expense authority administrators. We did not find an adequate process in place to inform these administrators of staff changes, creating a risk that approval levels are not updated promptly when there are changes in employment status, position or responsibility. We also found instances where the approval levels in Oracle Financials were inconsistent with those in the Corporate Signing Authorities System, which is the government's official register for recording the expense authority information for ministries.

- To ensure that purchases are authorized and goods and services are received, it is important that incompatible functions are properly segregated. Oracle Financials does not allow expense authorities to approve purchase transactions that they have entered. However, in some instances expense authorities can make changes to purchase orders—such as increasing quantities or changing delivery addresses—before approving them. Although changes can be made to purchase orders by the approver, the intent of the control is still being met, which is to ensure that the person entering the transaction is different from the person approving the expenditure. However, the strength of the control would be improved if changes to the purchase order required re-approval. We recommend that the feasibility of requiring approval by another expense authority be explored in these cases. Also, by policy, expense authorities and receivers for any purchases should not be the same people. We found that this policy was not always being followed.
- Because of the significant role played by expense authorities in authorizing expenditures, the approval information maintained in Oracle Financials should be easily retrieved and reported. As this was not the case, we recommend reviewing the feasibility of distinguishing expense authority approval from a non-expense authority action and recording the two differently in the Oracle tables.
- Purchase transactions appear to be adequately reviewed for approval by expense authorities to ensure the validity of transactions. However, we noted that there is a lack of guidance provided to expense authorities about the risks and significance of their review pertaining to:
  - the ability to make one-time address changes, possibly resulting in goods being redirected to unauthorized locations; and
  - the ability of expense authorities to approve purchases without knowing who the suppliers will be, possibly resulting in procuring goods and services from inappropriate suppliers.

Also of concern was the potential to make one-time address changes, redirecting suppliers' cheques to other addresses, possibly fraudulent ones, without the ability of expense authorities to review the addresses.

The recommendations concerning purchasing and accounts payable controls are listed in Appendix B.

Main findings

Ensuring access to create, change or cancel purchase requisitions, purchase orders and invoices is appropriately restricted to authorized individuals

For the ministries we reviewed, we found many instances where individuals were assigned incompatible responsibilities. There were examples of:

- employees assigned incompatible responsibilities that give them the ability to enter invoices and to force-approve invoices; and
- expense authorities assigned incompatible responsibilities giving them the ability to assign employees' approval levels in Oracle Financials or to enter requests for new suppliers or supplier changes.

Because expense authorities have the ability to both commit spending and approve purchases, it is important that these individuals be restricted from having the power to change their own approval level, set up new suppliers, or make changes to supplier information without requiring additional approval.

In our assessment of user access under the security administration section of this report, we make recommendations to ensure access granted remains appropriate based on users' positions. We also believe that access granted to users with expense authority should be reviewed periodically by ministries to ensure the Oracle responsibilities assigned to them are compatible with their roles as expense authorities.

Ensuring Oracle Financials approval levels are secured and configured in conformity with established business requirements

Policies and procedures concerning approval set-up

There are clear policies and procedures that establish accountabilities and responsibilities for the control and management of government expenses. The Comptroller General has overall responsibility for setting standards and maintaining government's financial policy framework.

Policy requires that only expense authorities can approve expenses from budgets that they have been given responsibility for. The purchase amounts that expense authorities can approve are limited by dollar thresholds and expense categories. The expense levels that positions can approve are pre-defined on a standard expense authority matrix known as the Common Expense Authority Matrix (see Exhibit 8).

Although this matrix is common to all ministries, each ministry can select approval levels suitable for their business environments, creating ministry specific matrices. These matrices, and any changes to them, must be approved by a minister or deputy minister. For the ministries we reviewed, we found that the matrices had been properly approved.

Exhibit 8

Common Expense Authority Matrix

Level	*1*	*2*	*3*	*4*	*5*
Purchases, Payments, Accounting Transfers (Subject to budget, central agency and ministry policies)	Full $	500k	250k	50k	5k
All STOBs	A	A	A	A	A
All STOBs, except Salaries and Benefits	B	B	B	B	B
All STOBs, except Government Transfers	C	C	C	C	C
Assets and Liabilities	D	D	D	D	D
Salaries and Benefits, and Operating Costs	E	E	E	E	E
Operating Costs	F	F	F	F	F
Government Transfers	G	G	G	G	G
Other Expenses	H	H	H	H	H
Revenues	I	I	I	I	I

Source: Core Policy and Procedures Manual, Ministry of Finance

The matrix defines the dollar limit and expense category (as defined by STOB ranges) that an expense authority or a position can authorize for a purchase. There are eight predefined ranges of STOBs and five predefined threshold levels. Each of the forty combinations of these two values corresponds to an approval level.

Ministries are also required to maintain their expense authority matrices on the Corporate Signing Authorities System (CSAS), a separate system not integrated with Oracle Financials. It is the government's official register for recording the ministry expense authority information.

Defining approval levels

Corporate Accounting Services is responsible for setting up the approval structure in Oracle Financials based on the ministry matrices. When expense authorities are assigned to predefined approval levels, it will allow them to approve requisitions, purchase orders or invoices up to a certain dollar limit and for certain account ranges.

We found that approval levels were properly set to allow ministry expense authorities to only approve transactions of their ministries, for their specified account ranges and dollar limits according to their ministry matrices.

To ensure only authorized approval levels were setup in Oracle Financials, we compared the defined approval levels for selected ministries to their respective approved ministry-specific expense authority matrices. We did not find any exceptions.

Update and approval procedures for changes to employee approval levels

The expense authority maintenance function is centrally administered in ministries and restricted to a few designated staff—known as expense authority administrators. They are responsible for assigning and updating employee approval levels in Oracle Financials. This maintenance is important to ensure the system correctly reflects the approval levels that employees with expense authority can authorize for payments.

The administrators are also responsible for updating the information to the CSAS system. Since the two systems are not linked, the expense authority information has to be separately updated.

Requests to set up employees as expense authorities or to change employees' approval levels are typically initiated in ministry program areas. Administrators first ensure that requests originate from appropriate senior officials in the program areas before updating the two systems.

We reviewed the approval and update processes for changes to employee approval levels at selected ministries. We found that the system does not prevent administrators from making changes to approval levels for employees of another ministry. We recommend Corporate Accounting Services determine the feasibility of restricting changes to employees within their own ministry.

Procedures are in place to ensure only authorized individuals with spending responsibilities are initially set up as expense authorities in the system. However, we are concerned about the ongoing maintenance of employee approval levels. There is an inadequate process to inform administrators of all staff changes on a timely basis. Administrators often rely on ministry program or business units to inform them of any staff changes. As a result, there is a risk that approval levels are not being promptly updated when there are changes in employment status, position or responsibility.

In our assessment of user access to Oracle Financials (see the security administration section of the report), we recommend that procedures be established to communicate staff changes to ministry security administrators in a timely manner to ensure effective user access change management.

We also recommend that the ministry expense authority administrators be informed of staff changes at the same time, to ensure the prompt update of employee approval levels.

Employee approval levels granted to expense authorities

Monitoring helps minimize the risk of someone approving payments when they do not have the authority to do so. We checked to see whether approval levels assigned to expense authorities in Oracle Financials were monitored periodically to ensure they remain current and relevant.

We ran tests comparing expense authority approval levels between Oracle Financials and CSAS data. We found instances where approval levels in Oracle Financials were inconsistent with those of CSAS.

We also reviewed the monitoring practices of selected ministries and found that some ministries we reviewed, developed their own reconciliation process to ensure consistency in approval levels between Oracle Financials and CSAS data. While a data comparison will provide them with some assurance on the accuracy of entries, it will not ensure that all approval level changes have been captured and properly set up in the system.

We recommend that monitoring procedures be established to periodically review the set-up of the expense authority approval levels in Oracle Financials, to ensure they remain current and appropriate.

Routing rules

Expense authority approvals can be temporarily assigned to alternates by the use of routing rules. These routing assignments automatically transfer the expense authority approval limits to designated alternates, so they can receive and act on all notifications for expense approval while the regular expense authorities are absent, such as for vacations. This temporary transfer of authority can be delegated only to those already established in the system as expense authorities or "trained expense authorities." We did not note any exceptions in our testing.

Ensuring payments are only made for authorized purchases and for goods and services received

Purchase authorization

All purchases of goods and services must be approved by an expense authority. To ensure transactions were being properly approved, we ran tests to check if there were any approved by expense authorities without the appropriate authority level. We did not find any exceptions and therefore concluded that the system is operating properly.

When goods are received or services are rendered, receivers certify their receipt. iProcurement does not allow invoices to be paid until receipts are recorded in the system. Our tests of iProcurement transactions confirmed this.

The requisition, purchase and invoice recording process

The purchasing process through iProcurement—from initial procurement through to receiving and invoice payment—involves a number of Oracle-defined job roles that are associated with different responsibilities. The key roles are: preparer, approver (expense authority), and receiver. A single person at a ministry may not occupy incompatible roles on the same transaction, as it is important that incompatible activities be separated to prevent fraudulent activities or errors going undetected.

Requisitioning process

During the requisitioning process, the preparer submits the requisition for approval.

The approver (expense authority) receives a "request for approval" notification (electronically), reviews the requisition and, if appropriate approves the requisition on-line. The preparer is then electronically notified that the requisition has been approved.

Purchasing process

During the purchasing process, only an approved requisition becomes a purchase order that is communicated to the supplier.

The supplier delivers the goods and services and the receiver enters receipt of goods, identifying quantity and amount received. Receivers are responsible for ensuring goods and services have been properly received or rendered—that is, they are as ordered, in the correct quantity, and any specified conditions met.

Invoicing process

During the invoicing process, the supplier invoices for goods and services delivered.

The accounts payable clerk enters and matches the invoice to the purchase order. (Until goods and services are received, no invoice against a purchase order can be paid.)

Segregation of functions to prevent expense authorities from entering and approving transactions

Oracle Financials has a system-enforced rule that prevents preparers (that enter transactions into the system) and expense authorities (that approve the transactions) from being the same people—as specified in the user guide. Expense authorities therefore cannot approve purchase transactions they entered. We tested this control and did not find any exceptions. However, we found that expense authorities with a certain combination of entry responsibilities could change requisition, purchase order or invoice details before approving them, without requiring additional approval. To prevent this, the system should require re-approval when expense authorities make changes to these procurement documents, especially if it would result in increasing the dollar amount or quantity or in changing accounting segments or the delivery address. We recommend that Corporate Accounting Services explore the feasibility of not allowing expense authorities to approve critical changes that they made directly to transactions.

Segregation of duties to prevent expense authorities from receiving goods or services for the transactions they approved

As previously mentioned, the approvers and receivers for any purchase transactions should not be the same people. The system, however, does not prevent this. We found instances where the expense authorities and the receivers were the same people. This is a policy requirement that must be enforced outside the system.

To assist ministry management in monitoring compliance activities for proper segregation of duties, Corporate Accounting Services developed a report that identifies approvers and receivers for all transactions. However, the usefulness of this report as a monitoring tool depends on whether the ministries are using the system to record the actual receiver.

Since receipt for transactions could be entered by those acting on behalf of receivers, the report may have limited value for detecting non-compliance. The usefulness of the report for monitoring non-compliance therefore depends largely on their business practices.

We recommend that ministries assess their business practices and implement appropriate monitoring activities for managing non-compliance over the segregation between expense authorities and receivers.

Capturing and retrieving approval information

Because of the significant role expense authorities play in authorizing expenditures, the approval information maintained in Oracle Financials should be easily retrieved and reported. As this was not the case, we recommend Corporate Accounting Services review the feasibility of distinguishing between expense authority approvals and non-expense authority actions and record them differently in the Oracle tables. Currently the table records certain acceptance actions as "Approvals" when they really were not expense authority approvals.

Ensuring key financial reports are reviewed and monitored to ensure validity, completeness and accuracy of recorded transactions

The electronic procurement approval process

When approving transactions, expense authorities are responsible for ensuring that expenses are properly charged against their budgets, that they do not exceed the available budgets, and they comply with all relevant statutes and policies. Exercising this authority therefore requires due care and diligence.

When a requisition, a purchase order or an invoice is submitted for approval, a notification is generated to advise the expense authority that an action is required to approve the transaction. The electronic link in the notification notice takes the user to Oracle Financials where the expense authority can logon to the system. Our review of the electronic procurement approval process has identified the following key concerns.

First concern: potential for the delivery of goods to an unauthorized location

When creating a requisition, the preparer must identify the location where goods are to be delivered. The location could be selected from a pre-defined list of government office addresses or, if not listed, the preparer could manually enter a different address. Having the ability to make a one-time address change creates an opportunity for goods to be redirected to an unauthorized location. It is therefore important that any manual overrides are subject to the review and approval of the expense authority.

Although the one-time delivery location change entered by the preparer could be viewed by the expense authority, this review was not always carried out. We noted that there is a lack of guidance provided to expense authorities about the risks and significance of their review on the one-time delivery location change, and the procedures that should be carried out to validate the change.

We recommend that guidance be established to address this concern.

Second concern: potential redirection of cheques to a fraudulent mailing address

When invoice payments to suppliers are processed in the accounts payable module, the suppliers' cheque mailing addresses are taken from the supplier table. Although suppliers' names cannot be changed, their addresses could be overridden thereby redirecting suppliers' cheque payments to other addresses. The address field is not available to expense authorities to view when approving invoices online. As a result, there is a risk that cheque payments could be redirected to fraudulent addresses.

We recommend that Corporate Accounting Services explore the feasibility of requiring approval from expense authorities when manual changes are made to suppliers' cheque mailing addresses, to prevent unauthorized changes. Guidance should also be established to ensure that proper validation procedures be carried out when approving changes.

Third concern: potential procurement from inappropriate suppliers

When preparing requisitions, staff are not required to identify suppliers with whom orders will be placed, as sourcing may not be known at the time. The supplier information, once identified,

is added to the purchase order but does not require expense authorities to approve it again. As a result, they may not know who the supplier is when approving the expenditures. Since expense authorities are accountable for all purchases, we think it is important for them to approve suppliers at the time orders are placed to avoid procuring goods and services from inappropriate suppliers who may contravene the government's procurement standards.

We recommend that management require expense authorities to review procurement transactions when supplier information is subsequently added to purchase orders or changed.

Responsibility for ensuring validity, completeness and accuracy of recorded transactions

As we have mentioned, ministries are responsible for complete and accurate transaction recording in Oracle Financials. There are clear policy requirements setting out the responsibilities that expense authorities have for reviewing financial management reports to ensure charges made to their program areas are complete and accurate.

Reports with varying levels of detail are available to all ministries, and are reviewed by several levels of staff. Typically, expense authorities review reports containing the transactions they approved, while another level of management reviews program area reports that include transactions approved by multiple expense authorities, and yet another level of management reviews branch reports that include several program areas.

Each level of review could potentially detect different conditions resulting from different risks. For example, the risk that CAS support staff with full system access could enter a fraudulent transaction or the risk that expense authorities could put through fraudulent transactions, could be caught at various levels of monitoring. However, for monitoring to be effective in detecting such transactions, the risks must be understood by those responsible for the reviews. We found that the expense authorities and the managers responsible for monitoring were not sufficiently aware of the risks that their reviews were supposed to be monitoring.

Because the monitoring within ministries is done differently, we could not determine whether the reviews in all areas were reasonable. We did conclude, however, that in the areas we looked at, the approach used for conducting the reviews was reasonable for what they were intended for.

We recommend that the Office of the Comptroller General take on the initial responsibility of communicating with ministries the risks of potential fraud in purchasing and accounts payable transactions and advising them on how to detect the potential threats resulting from these risks.

Review and approval of force-approved transactions

Force-approval is a powerful function that grants users the privilege to approve invoices for payments. It is used when the selected expense authorities are not available to do online approvals. Force-approved invoices do not have all of the key edits that normally apply to transactions when expense authorities approve invoices. For example, there are no edits to check that the person entering the invoice is not the same person approving the invoice, that the person approving the invoice has sufficient approval level to approve the dollar amount of the transaction, or that the invoice matches the amount of the associated purchase order.

Since those doing the force approvals online are not acting in the capacity of expense authorities, manual payment approval by appropriate expense authorities must still be applied to invoice payments. Ministries have procedures that specify the limited conditions when force approval transactions can be used.

For selected ministries, we reviewed the appropriateness of the business process for handling force-approved transactions. We believe that regular monitoring of the use of this type of approval should be carried out to make sure that, when it is used, proper manual expense authority approval has also been applied. We found that such monitoring is generally not done because for the most part ministries are not using force approval. Nevertheless, we recommend that they still monitor to ensure there were no occurrences.

Response from the Ministry of Finance and the Ministry of Labour and Citizens' Services

Response to the Audit of Government's Corporate Accounting System: Part 2

Introduction

We appreciate the opportunity to respond to the content of the detailed Corporate Accounting System Part 2 audit ('the audit'). Corporate Accounting Services (CAS) and the Office of the Comptroller General (OCG) are pleased with the Deputy Auditor General's conclusion that with some exceptions, proper control procedures are in place and being followed to ensure that financial information is processed completely, accurately and on a timely basis, for example:

- Security over governments accounting system is well managed
- Controls over data entry, processing, validation and management were working effectively
- Controls over access for the purchasing and accounts payable modules were for the most part appropriate

The report provides a comprehensive look at the payment process from end to end and is also the first complete review of purchasing since the implementation of the new control framework and iProcurement module of the Oracle Financial System beginning in 2004. Government has and is taking action to address the eleven key recommendations to address control issues found during the audit, as well as the more routine recommendations that will help us further enhance the control framework. This is consistent with the approach taken to address the recommendations put forward in the Corporate Accounting System Part 1 audit. All of the recommendations from the Part 1 audit have now been addressed, with one final item to be completed in October 2006.

The Control Environment

A strong control environment is important to CAS, OCG and ministry management. The BC Government, through the OCG, has a strong financial control framework in place which uses policy and procedures to augment financial system controls. The financial framework stems from legislation expanded through policy, and

includes system and manual controls, employee standards of conduct (ethics), as well as ministry and central post-payment review.

A key element of the financial framework is the role of the Senior Financial Officer who has a mandate to enforce policy and be accountable for maintaining effective controls. Expense Authority training and accountability is core to this responsibility. Staff with delegated Expense Authority have overall responsibility for the expenditures they sign-off, Qualified Receivers certify when goods are received, and post-audit reports are available to identify anomalies and exceptions. Exceptions are generally found to be supported by valid business reasons and adequate compensating controls are in place to reduce the risk of error, fraud or loss to a low level.

Response to Key Recommendations

The audit was conducted over an extended period of time in an environment that was undergoing active development and enhancement. The work on the audit began nearly two years ago, and since that time there have been a number of changes to both CAS Oracle (the financial system) and to the control framework, including the policies and governance required to support the financial system. The financial system has undergone a number of upgrades including a major version release in June of 2006. Many of the recommendations identified in this audit have been addressed as a result of this activity.

We have responded to the audit's key findings and recommendations at a summary level by four topical groupings below: security administration controls; general ledger controls; supplier maintenance controls; and, purchasing and accounts payable controls. We have also responded in detail to each of the individual recommendations.

Security Administration Controls

Security over access to the system is a key control. Ministries play an important role in ensuring access profiles in CAS are accurate and appropriately meet the business requirements of positions. When employees change positions or leave government, the respective ministries are to advise CAS of the changes so that

the employee may perform the duties of their new position. If the employee has left government, security controls prohibit access from outside the government network.

Working with ministries and the OCG, CAS will identify access profile combinations that could potentially create risk in the system, and review the feasibility of creating exception reports and implement a process to regularly clean up user responsibilities.

General Ledger Controls

OCG will formalize its existing monitoring, verification and year end procedures to ensure chart of accounts data that support financial reporting is accurate and complete and the required reconciliations are performed by ministries. The remainder of the recommendations will be addressed though regular communication with ministry financial staff both informally through the Senior Financial Officer Committee, the Financial Officer Advisory Committee and formally through annual training sessions.

Supplier Maintenance Controls

OCG has reiterated with ministry financial staff and supplier maintenance contacts that changes to supplier contact and related banking information must be independently verified and documented to ensure the validity, and accuracy of the information, as well as, ensuring the requestor has the authority to make the change.

CAS currently requests documentation to support changes to supplier data, verifies supplier changes against the Corporate Registry and no longer allows the creation of generic suppliers.

The other recommendations related to supplier maintenance will be addressed in two projects already underway by CAS and OCG, the Supplier Management Project and the Block and Generic Supplier Review.

Response from the Ministry of Finance and the Ministry of Labour and Citizens' Services

Supplier Management Project – CAS

In June 2006 CAS initiated a project to perform a comprehensive review of supplier management. Following the review of the recommendations in this audit, each recommendation related to supplier and banking information management is now addressed within the scope of this project.

Block and Generic Supplier Review – OCG

The use of block supplier coding is currently required in a few selected government business processes and does carry additional risk compared to general and employee supplier coding. OCG is currently reviewing mitigation or alternate strategies with the desire to reduce overall risk while permitting administrative efficiencies where the practice will need to be continued. In the short term OCG is reviewing existing block supplier usage, policy for when a block supplier code can be used, assigning risk ratings, and developing system control enhancements. This will also ensure that the few additional payments to suppliers over $25,000 are fully reported.

Purchasing and Accounts Payable Controls

In order to ensure the effectiveness of the expenditure authority review of transactions as well as financial management reports, OCG will be updating existing Expense Authority training material to highlight the potential risks associated with purchase transactions. Training will re-emphasize the importance of regular reviews of financial management reports available from CAS and identify what each level of review is to accomplish. Additional training will be made available to ministry staff.

The next section provides a detailed response to each recommendation in the audit.

We appreciate the time taken in conducting the audit and in preparing this report. We look forward to working with the Office of the Auditor General in the future to ensure the effectiveness of the financial framework and its related controls.

Response from the Ministry of Finance and the Ministry of Labour and Citizens' Services

Detailed Response to Recommendations

Security Administration Controls

1. **We recommend that a review be performed to determine whether users and support staff allowed to login directly to the accounting system, bypassing the single sign-on process, still require this access.**

   This control has already been implemented by CAS by limiting direct access to the system to database administrators who need this access to do their jobs. A list of such access is maintained by the Security Officer. Any temporary access required during project implementations or emergency maintenance must be approved by the Security Officer or designate (Technology Operations Director) and immediately removed after completion of the project or maintenance.

2. **To comply with the government security policy, we recommend that Corporate Accounting Services set the Oracle Financials user profile option so that passwords must contain alpha and numeric characters, be a different value from the userid and have an expiry date.**

   This control is being reviewed for implementation by CAS and is currently undergoing internal testing prior to release into the production system.

3. **To ensure the effectiveness of the Security Officer position, we recommend that the responsibilities and authority extend across all departments in Corporate Accounting Services and the role is clearly documented to reflect this authority.**

   This control has already been implemented by CAS. The responsibilities and authority of the Security Officer extend across all departments and the role is clearly documented to reflect this authority.

   The mandate of the Security Officer was clearly communicated to existing staff through mandatory training sessions. New staff, including both staff and contractors, are educated about this role through the CAS Orientation Manual and staff orientation

sessions. There is ongoing communication between the Security Office and the CAS staff through electronic mail bulletins and use of the CAS internal web-site.

The Security Officer has the authority to bypass the Director and/or the Executive Director and go straight to the Assistant Deputy Minister (ADM) if deemed necessary.

4. **Although the ultimate responsibility for user access lies with each ministry, as Corporate Accounting Services staff have valuable knowledge of CAS and its various tools (such as exception reports) we recommend that they take a more proactive role in ensuring all access is appropriate by using their knowledge and tools to alert ministries of possible problems with user access.**

   CAS will provide ministry security contacts with detailed information on the functionality available in each system responsibility.

   CAS will also provide a matrix of possible combinations of responsibilities that could potentially create a risk in the system e.g. an expense authority having the ability to add a supplier.

   CAS will determine the effort to implement this recommendation within the current fiscal year.

5. **We recommend that procedures be established to communicate staff changes to the security administrators in a timely manner to ensure effective user access change management, and to periodically review user access levels to ensure access granted remains appropriate based on users' positions.**

   CAS will share its established exit procedures with ministries to ensure the step to notify the ministry security contact is included.

   CAS will also create exception reports based on active ID's in the Government electronic mail directory matched against the user base in Oracle. Cleanup could then be performed on a regular basis, with notification to ministry contacts regarding any exceptions.

   CAS will determine the effort to implement this recommendation within the current fiscal year.

6. **We recommend that the Security Officer at Corporate Accounting Services monitor the table that contains data on failed login attempts.**

   This control has already been implemented. CAS currently monitors the CAS Portal login table daily and invalid login attempts to the direct URLs hourly.

   Single Sign On login attempts are captured at the Common Logon Page (CLP). The BC government network logon rules apply to these logon attempts and the ID is frozen after 3 tries.

7. **We recommend that Corporate Accounting Services review accesses identified during our audit where there was a question as to whether the access was still required, and remove any unneeded accesses.**

   CAS has reviewed the access identified in this audit and removed unneeded accesses. Access levels are currently monitored on a regular basis, identifying and removing access no longer required. Access may be granted for project implementations and post implementation support and is removed once the business need for this access has ended.

8. **To ensure that profiles with security implications conform to policy, we recommend that the Security Officer be consulted when determining the values issued to security settings.**

   CAS will incorporate this as a step in the operating procedures used to deliver projects at CAS. This will be communicated to the Project Delivery Office and added to CAS documentation.

General Ledger Controls

Chart of Accounts Maintenance

9. **We recommend that procedures be established to monitor the appropriateness of the segment access rules. Segment access rules should be periodically reviewed for any missed segment value ranges or overlapping ranges that have been created in error.**

   OCG has implemented this control and has established routine verification processes to ensure all active service line values have assigned rules. In this case the risk is minimal as a segment cannot

be used unless an access rule has been assigned. It is agreed that segment values no longer required should be disabled. OCG will work with CAS to identify overlapping ranges.

There are often valid business reasons to have multiple ministries access a segment value, such as during the annual budget cycle, or as an interim measure when ministries are re-organized.

10. **To provide a proper audit trail, we recommend that procedures be established requiring supporting documentation to be maintained for all segment value changes to the chart data.**

    OCG has already implemented this control and has initiated a monitoring system for all change requests used to track all changes including spelling and punctuation. In addition, supporting source documentation is kept for all change requests to ensure there is an audit trail. Comparisons of periodic reports of the master listings to chart master data has been undertaken to assure completeness and accuracy.

11. **We recommend that ministries periodically review the cross validation rules defined for their ministry to ensure the rules are set appropriately for their business, allowing proper validation to take place.**

    OCG has already implemented this control by adding this to the year-end tasks ministries should be completing in late February of each year. Additionally, there are occasional reviews completed by CAS.

12. **We recommend that monitoring activities be formalized and carried out by Office of the Comptroller General (OCG) to ensure the chart data remains current and relevant.**

    OCG has already implemented this control by incorporating the routine monitoring of the chart master database into monthly tasks to ensure it remains up to date and accurate.

Response from the Ministry of Finance and the Ministry of Labour and Citizens' Services

Journal Processing

13. **Because using the responsibility for inter-ministry journals to enter intra-ministry journals increases the risk of data entry errors, we recommend that management evaluates this risk versus the gain in efficiencies.**

    OCG will review risk versus efficiency to determine if separate procedures for inter and intra-ministry journal entries are warranted.

14. **We recommend that ministries review their needs and requirements, and determine if they could benefit from the use of recurring or allocation journals to allow for more efficient and effective journal processing.**

    This control has been implemented by OCG in that the automation of allocation journals is currently available to ministries, however set up and administration is resource intensive and has not been seen as sufficiently effective to warrant implementation. There are no policy impediments for expanded use of recurring or allocation journals.

15. **To ensure that all journal batches are clearly distinguished, we recommend that ministries adhere to the established batch naming convention when creating journal batches in Oracle Financials general ledger.**

    It is the responsibility of the ministries to adhere to established naming conventions. CAS and OCG will stress the use of existing naming conventions through training and communication.

16. **We recommend that ministries review their journal processing process to ensure proper procedures are in place to prevent duplicate journal entries.**

    It is the responsibility of ministry Expense Authorities to review financial transactions and charges to their area of responsibility. This includes journal entries into the general ledger. This recommendation will be conveyed to the Financial Operations Advisory Council for further communication at the ministry level.

Response from the Ministry of Finance and the Ministry of Labour and Citizens' Services

Reconciliation and Financial Reporting

17. **We recommend that a reconciliation procedure be established to provide OCG management with the necessary assurance that the data in CODE is complete, accurate and timely and reflects the data in the Oracle Financials production system.**

    CAS conducts over 200 daily reconciliations to ensure that the data in the data warehouse is complete, accurate, timely, and reflects the data in the financial system. These reconciliations are reviewed daily.

    OCG management will establish a routine review of the results of these reconciliations to gain assurance that the data in the data warehouse is complete, accurate, timely, and is reflective of the data in the financial system.

18. **We recommend that OCG communicates clearly to ministries the responsibility and requirement for reconciling the liability balance as reported in the Oracle Financials accounts payable subsidiary ledger to the general ledger.**

    OCG has implemented this control and instructs ministries through monthly, quarterly and year-end reporting communications. The importance of reconciliations, and how to perform reconciliations, is presented by OCG to ministries through our annual training programs.

19. **We recommend that ministries maintain a reconciliation schedule to ensure all accounts are reconciled and to allow management to oversee the month-end reconciliation process.**

    OCG has implemented this control by requiring ministries to signoff on all balances except inter-ministry and Consolidated Revenue Fund (CRF) cash each quarter. The importance of reconciliations, and how to perform reconciliations, is presented by OCG to ministries through our annual training programs.

    CAS is also in the process of assisting ministries with this control under the recently completed CAS Reporting and Information Strategy. The strategy recommends moving towards role-based

reporting. This entails presenting reports by job function. This approach will be used to standardize reports and processes required for sub-ledger and month-end reconciliation.

Supplier Maintenance Controls

20. We recommend that procedures be established to identify suppliers with missing address information, and update them accordingly.

CAS has identified this issue and the supplier management project currently underway will investigate the feasibility of cleansing incomplete address information.

It is important to note that the majority of the missing address information was created in the legacy financial system and later converted into the current system. There are system edits in the current financial system to ensure the completeness of address information.

21. We recommend that procedures be established requiring a copy of the supplier invoice or other documentation supporting the requested change be forwarded to the Ministry supplier maintenance person to ensure accuracy and validity of the information entered to the supplier table.

CAS currently requests documentation to support a change to supplier data if the change cannot be verified from other sources such as the corporate registry or the company web-site.

OCG will communicate the requirement to ensure adequate documentation is in place to support supplier information in CAS.

22. We recommend that verification procedures be strengthened to include a search on supplier addresses to assist in identifying whether the supplier already exists in the supplier table.

CAS has investigated this control and this functionality is not currently available in the financial system. The cost of implementing a custom solution may be prohibitive, however the feasibility will be investigated within the scope of the supplier management project currently underway.

23. To promote effective supplier searches, we recommend that Corporate Accounting Services identify and correct all supplier names and addresses of existing records that have not been formatted according to the standard naming and addressing conventions.

CAS has also identified this control and will investigate the feasibility of a supplier data cleanse within the scope of the supplier management project scheduled for the fall of 2006. CAS is implementing a data cleanse of the customer data in October 2006.

24. We recommend that Corporate Accounting Services reinforce with ministry staff the importance of following the standard naming convention when entering new supplier information, and verifying the entries to supporting documents for accuracy.

CAS will issue a communication within the current fiscal year to ministry staff stressing the importance of following the standard naming conventions and of verifying entries. As well, this message will be reinforced in any training, documentation or supporting material which refers to supplier setup.

25. We recommend that Corporate Accounting Services reinforce with its staff the importance of checking the entered supplier information for compliance and establish periodic review procedures to ensure that the naming and addressing conventions are being complied with.

CAS support staff currently perform a detailed review of supplier information for compliance with procedures and naming conventions prior to the supplier set-up being finalized. CAS will reinforce the importance of this process with staff and will review the supplier data as part of the supplier management project.

26. We recommend that monitoring activities be established to ensure the supplier data remains current and relevant.

CAS will investigate the options and feasibility of implementing this control under the supplier management project.

27. **To maintain data integrity, we recommend that Corporate Accounting Services periodically review the supplier table to identify duplicate suppliers and deactivate them accordingly.**

    CAS will investigate the options and feasibility of implementing this control under the supplier management project.

28. **We recommend that Corporate Accounting Services explore the feasibility of carrying out a data matching process, comparing the supplier information to that of the provincial Corporate Registry, so supplier records can be updated to reflect current information.**

    CAS has implemented this control and currently manually verifies supplier changes against the Corporate Registry. The feasibility of automating this process, and the costs associated with this automation, will be addressed through the supplier maintenance project.

29. **To facilitate this data matching, we recommend that procedures be established to require the collection of the business registration numbers for all new business suppliers, and when practical, for existing business suppliers as well.**

    The feasibility of implementing this requirement will be investigated within the supplier management project.

30. **We recommend that Corporate Accounting Services establish formal policies restricting further set-up of generic suppliers and formalize a plan to establish a well-defined approach for using, managing and updating existing generic supplier records.**

    CAS has implemented this control and generic suppliers are no longer created. CAS will formalize a plan to remove any remaining generic suppliers.

31. **We recommend that OCG establish clear policies and guidelines for the ministries, to guide them when using block suppliers in processing payments.**

    This will be addressed in the OCG's overall assessment of block supplier coding.

32. **We recommend that OCG establishes clear criteria for monitoring and compliance activities to ensure that the block supplier data remains current and relevant.**

This will be addressed in the OCG's overall assessment of block supplier coding.

33. **We recommend that an assessment be carried out to identify all high-risk block supplier payment types where the potential exposure of the payee could compromise confidentiality and privacy and appropriate procedures be established to ensure proper processing of these payments with due regard to confidentiality of information.**

This will be addressed in the OCG's overall assessment of block supplier coding.

It is a priority of CAS and OCG to ensure the appropriate levels of confidentiality and privacy are exercised through policy and performance standards.

34. **We recommend that policies and procedures be established to define clearly the ministry's role and responsibilities in the bank account maintenance process, and to govern the extent of ministry review required for ensuring the completeness and accuracy of banking information obtained.**

CAS will work with Provincial Treasury to investigate the options available. Bank account maintenance is within the scope of the supplier management project.

35. **We recommend that control procedures be strengthened to ensure accuracy and completeness of bank account change information originated from the supplier, an important measure to ensure authenticity of the supplier.**

OCG has communicated the requirement to verify the changes to supplier contact and banking information with existing supplier files and through a separate contact back to the supplier.

36. We recommend that OCG effectively communicate to the ministries the risks associated with banking activities and advise them of how to detect the potential threats and to ensure that controls are functioning properly to address them.

OCG has communicated the risks associated with changes to banking information to the financial community. The issue has been discussed at both the Senior Financial Officer Council and the Financial Officer Advisory Committee.

37. We recommend that management at Corporate Accounting Services formalize procedures to monitor all supplier linkages to bank accounts and compare the details of the reported link activities to the source documents to ensure that there is no unauthorized or inappropriate bank account linkages.

CAS will work with Provincial Treasury to investigate the options available. Bank account maintenance is within the scope of the supplier management project.

38. We recommend that procedures be established to periodically review the bank account information for suppliers with multiple sites to ensure that they take on the same bank account details on each of their sites.

CAS will work with Provincial Treasury to investigate the options available. Bank account maintenance is within the scope of the supplier management project. This business process may change as a result of this review.

39. We recommend that periodic review procedures be established to ensure that bank accounts that have not been flagged for multiple supplier assignment, are not assigned to more than one supplier.

CAS will work with Provincial Treasury to investigate the options available. Bank account maintenance is within the scope of the supplier management project.

40. We recommend that management determine if retention of electronic payment request forms is required and if so that the required copies are retained in locked cabinets.

CAS will work with Provincial Treasury to investigate the options available. Bank account maintenance is within the scope of the supplier management project.

Purchasing and Accounts Payable Controls

41. We recommend that access granted to users with expense authorities be reviewed periodically to ensure the Oracle Financials responsibilities assigned to them are compatible with their role as expense authority.

OCG will communicate the responsibility of Senior Financial Officers to support their Deputy Ministers in expense authority table maintenance.

42. We recommend that Corporate Accounting Services determine the feasibility of restricting expense authority administrators to only assigning approval levels to employees within their own ministry.

CAS has investigated implementing this as a system control and has determined that the functionality to restrict the expense authority administrators to assigning approval levels within their own ministries would be a customization to the financial application. Besides being cost-prohibitive, there are valid business reasons for allowing cross-ministry approval level assignments, such as when the centralization of cross-ministry financial services occurs. As an example, the Ministry of Finance currently provides central accounting services to other ministries and agencies such as the Ministry of Labour & Citizens' Services and the BC Public Service Agency.

As a compensating control, ministry Senior Financial Officers have the responsibility to monitor ministry approval levels and recommend expense authority delegations.

43. We recommend that ministry expense authority administrators be informed of staff changes at the same time as security administrators, to ensure prompt update of necessary changes to employee approval levels.

OCG agrees and will review ministry procedures to determine if there is a viable technical solution from information contained in the HR system. OCG will engage Financial Officer Advisory Committee (FOAC) to determine a government direction for updating staff action notifications to always include the expense authority administrators.

44. We recommend that monitoring procedures be established to periodically review the setup of the expense authority approval levels in Oracle Financials to ensure that the approval levels assigned to expense authorities remain current and appropriate.

OCG agrees and will review ministry procedures and engage BC Public Service Agency (PSA) to determine if there is a viable technical solution for expense authority administrators to obtain information contained in the HR System. OCG will engage FOAC to determine a government direction for updating staff action notifications to always include the expense authority administrators and for ministry branch heads to review their organizational requirements.

45. We recommend that Corporate Accounting Services explores the feasibility of not allowing the expense authorities to approve critical changes that they made directly to a transaction.

OCG has explored this control and have determined that it is within the financial framework to allow for expense authorities to approve certain changes they have made.

The controls in the financial system are designed to provide the segregation of duties between the preparer, the expense authority, and the qualified receiver.

Under the control framework, the responsibility to authorize expenditures for both spending and payment has been shifted to one official. It is the prerogative of the expense authority in this situation to make the changes as they are accountable for all purchases they approve.

The enforcement of policy and the post audit review of approval activity are considered adequate controls to support the control framework.

46. We recommend that ministries re-assess their business practices and implement appropriate monitoring activities for detecting and managing non-compliance over the segregation between an expense authority and a receiver.

As part of the implementation of the iProcurement module, ministries submitted Risk and Controls Reviews to OCG detailing compensating controls they had put in place to effectively manage and detect non-compliance.

Additionally, CAS and OCG have implemented financial management reports that specifically identify any actual or potential non-compliance (Expenditure Authority = Qualified Receiver). Post payment review also has procedures to identify potential segregation issues.

OCG will request that ministries review their existing controls to ensure their ongoing processes adequately ensure proper segregation of duties.

47. We recommend Corporate Accounting Services review the feasibility of distinguishing an expense authority approval versus a non-expense authority action and record them differently in the Oracle tables.

CAS currently makes reports available to ministries and the Payment Review Office that separate out the true expense authority approver from other approvers. CAS will work with ministries and the OCG to review the feasibility and need for further information breakdown or table changes.

In addition, CAS works with the Payment Review Office and the financial system support resources to ensure that the action histories recorded in the system clearly define the events that have occurred.

48. **We recommend that guidance be established to ensure expense authorities are aware of the risks of manually changing addresses where goods are to be delivered, and that proper validation procedures be carried out approving these changes.**

Expense authority training will be updated to acknowledge this recommendation. However, addresses for delivery are not considered a critical field for Expense Authority and validation occurring with the Qualified Receiver is deemed an appropriate control. This process relies on the Expense Authority / Qualified Receiver roles to ensure compliance.

49. **We recommend that Corporate Accounting Services explore the feasibility of requiring approval from expense authorities when manual changes are made to suppliers' cheque mailing addresses, to prevent unauthorized changes. Guidance should also be established to ensure that proper validation procedures be carried out when approving changes.**

This control will be investigated as bank account maintenance is within the scope of the supplier management project.

50. **We recommend that management require expense authorities to review procurement transactions when supplier information is subsequently added to purchase orders or changed, to ensure appropriateness of the suppliers used for procuring the goods and services.**

OCG has determined the enforcement of policy and the post audit review of approval activity are considered adequate controls to support the control framework.

The expenditure authority is within their authority to make changes to the purchase order prior to approval. The key controls over the purchase are the qualified receiver's certification of what was ordered was received and the three-way matching of goods ordered and received to the supplier invoice. In many cases buyer specialists manage this process and deal directly with the supplier community to select the appropriate supplier for goods or services. There are controls in place to preclude changes that increase the dollar limits of transactions over pre-approved limits.

Response from the Ministry of Finance and the Ministry of Labour and Citizens' Services

51. We recommend that OCG take on the initial responsibility of effectively communicating with ministries the risks of potential fraud in purchase and accounts payable transactions and advising them on how to detect potential threats resulting from these risks.

OCG agrees that the expense authority must be supported by having access to the information available to them. OCG, through FOAC and input into the expense authority training syllabus, will continue to promote education and understanding of the accountability of the expense authority role, including the risks of loss or misappropriation.

52. We recommend that ministries regularly monitor reports for force-approved transactions to ensure that there are no occurrences and when there are occurrences, all transactions are appropriate and have received expense authority approvals.

Force-approval is a transitional function, permitted by policy, as ministries align legacy systems and manual processes to the control framework. OCG requires ministries to apply to use force-approval, detailing compensating controls and strategies to discontinue the reliance of the function. Force-approval has very limited ministry uptake and is reviewed continually by the Payment Review Office and the Financial Management Branch as well as ministries through specifically designed reports.

OCG as part of expense authority training and through communication with Senior Financial Officer Council and Financial Officer Advisory Committee will require ministries who do not require force-approval functionality to periodically review available force-approval reports to ensure it has not been used.

Appendices

Appendix A: History of Changes to Government's Corporate Accounting System (CAS)

Year	Corporate Accounting System (CAS)							Office of the Auditor General Audits
	General Ledger (GL)	Accounts Payable (AP) and Purchases	Accounts Receivable (AR)	Fixed assets	Data warehouse	Operating environment	Other	
1998	Oracle Financials pilot (implementation of GL, AP, purchase order modules for 2 pilot ministries)							
1999	Oracle Financials implementation of piloted modules for all ministries; transactions also entered into the old (Walker) system		Oracle Financials AR implemented for 1 ministry and 1 Crown corporation					
2000	Common chart of accounts implemented for all ministries				Data warehouse implemented for all ministries. (Minimal usage: still using old system.)			
2001	Walker system decommissioned; Oracle Financials now Corporate Accounting System	Oracle Financials iExpenses pilot (entry of travel expenses by employees)		Oracle Financials fixed assets module pilot by 2 ministries	Data warehouse standard reporting for all ministries		Payment Review Office created	
		iExpenses implemented for all ministries						
2002	Treasury Board approval; Corporate Accounting System Initiative within $1,000 vote of Solutions BC			Oracle Financials Fixed Assets module implemented for all ministries				**Review of UNIX operating environment**

Appendix A: History of Changes to Government's Corporate Accounting System (CAS)

Year	Corporate Accounting System (CAS)							Office of the Auditor General Audits
	General Ledger (GL)	Accounts Payable (AP) and Purchases	Accounts Receivable (AR)	Fixed assets	Data warehouse	Operating environment	Other	
1998	Oracle Financials pilot (implementation of GL, AP, purchase order modules for 2 pilot ministries)							
1999	Oracle Financials implementation of piloted modules for all ministries, transactions also entered into the old Walker system		Oracle Financials AR implemented for 1 ministry and 1 Crown corporation					
2000	Common chart of accounts implemented for all ministries				Data warehouse implemented for all ministries (Minimal usage, still using old system)			
2001	Walker system decommissioned. Oracle Financials now Corporate Accounting System	Oracle Financials iExpenses pilot (entry of travel expenses by employees)		Oracle Financials based assets module pilot by 2 ministries	Data warehouse standard reporting for all ministries		Payment Review Office created	
		iExpenses implemented for all ministries						
2002	Treasury Board approval: Corporate Accounting System Initiative within $3,000 cost of Solution; BC			Oracle Financials Fixed Assets module implemented for all ministries				Review of UNIX operating environment

Appendix A: History of Changes to Government's Corporate Accounting System (CAS)

Year	Corporate Accounting System (CAS)							Office of the Auditor General Audits
	General Ledger (GL)	Accounts Payable (AP) and Purchases	Accounts Receivable (AR)	Fixed assets	Data warehouse	Operating environment	Other	
2003	New Budgeting and Chart of Accounts Maintenance implemented for all ministries	Oracle Financials iProcurement module pilot with 2 ministries		Fixed assets available to 21 organizations		Oracle Financials 11i upgrade provides technical foundation for future initiatives	Corporate Accounting System initiative moved to Ministry of Management Services. Name changed to Corporate Accounting Services.	**Audit of CAS Oracle database**
2004		Oracle Financials iProcurement implemented for all ministries					Single sign-on implemented for CAS Oracle Financials, data warehouse and self-service modules for all users	**Review of CAS IT governance and follow-up on prior audits**
							Self service functionality for all ministries	
2005		Oracle Financials eProcurement Phase 2 implemented for all ministries			CODE Data Warehouse Upgrade	Replacement and upgrade of CAS servers and UNIX operating system		**Audit of Oracle Financials GL, AP and Purchases Modules**

Source: Solutions BC Newsletter, Ministry of Management Services

Appendix A: History of Changes to Government's Corporate Accounting System (CAS)

Year	Corporate Accounting System (CAS)							Office of the Auditor General Audits
	General Ledger (GL)	Accounts Payable (AP) and Purchases	Accounts Receivable (AR)	Fixed assets	Data warehouse	Operating environment	Other	
2003	New Budgeting and Chart of Accounts Maintenance implemented for all ministries	Oracle Financials iProcurement module pilot with 2 ministries		Fixed assets available to 21 organizations		Oracle Financials 11i upgrade provides technical foundation for future initiatives	Corporate Accounting System initiative moved to Ministry of Management Services. Name changed to Corporate Accounting Services.	**Audit of CAS Oracle database**
2004		Oracle Financials iProcurement implemented for all ministries					Single sign-on implemented for CAS Oracle Financials, data warehouse and self-service modules for all users	**Review of CAS IT governance and follow-up on prior audits**
							Self-service functionality for all ministries	
2005		Oracle Financials eProcurement Phase 2 implemented for all ministries			CODE Data Warehouse Upgrade	Replacement and upgrade of CAS servers and UNIX operating system		**Audit of Oracle Financials GL, AP and Purchases Modules**

Source: Solutions BC Newsletter, Ministry of Management Services

Appendix B: Summary of Recommendations

Security Administration Controls

Ensuring Oracle Financials security and control settings are adequately defined.

1. **We recommend** that a review be performed to determine whether users and support staff allowed to login directly to the accounting system, bypassing the single sign-on process, still require this access.

2. To comply with the government security policy, **we recommend** that Corporate Accounting Services set the Oracle Financials user profile option so that passwords must contain alpha and numeric characters, be a different value from the userid and have an expiry date.

Ensuring the security administration function is defined and assigned, and security administration policies and procedures exist to ensure adequate change management of user access.

3. To ensure the effectiveness of the Security Officer position, **we recommend** that the responsibilities and authority extend across all departments in Corporate Accounting Services and the role is clearly documented to reflect this authority.

4. Although the ultimate responsibility for user access lies with each ministry, as Corporate Accounting Services staff have valuable knowledge of CAS and its various tools (such as exception reports) **we recommend** that they take a more proactive role in ensuring all access is appropriate by using their knowledge and tools to alert ministries of possible problems with user access.

5. **We recommend**that procedures be established to communicate staff changes to the security administrators in a timely manner to ensure effective user access change management, and to periodically review user access levels to ensure access granted remains appropriate based on users' positions.

Ensuring access to data is appropriately restricted and monitored.

6. **We recommend**that the Security Officer at Corporate Accounting Services monitor the table that contains data on failed login attempts.

Appendix B: Summary of Recommendations

Ensuring users only perform compatible functions.

7. **We recommend** that Corporate Accounting Services review accesses identified during our audit where there was a question as to whether the access was still required, and remove any unneeded accesses.

Ensuring system profiles are adequately defined, access to them is restricted and changes are monitored.

8. To ensure that profiles with security implications conform to policy, **we recommend** that the Security Officer be consulted when determining the values issued to security settings.

Ensuring access to system output is appropriately restricted.

No recommendations were required.

General Ledger Controls

Chart of Accounts Maintenance

Ensuring additions and changes to the chart of accounts are valid.

9. **We recommend** that procedures be established to monitor the appropriateness of the segment access rules. Segment access rules should be periodically reviewed for any missed segment value ranges or overlapping ranges that have been created in error.

Ensuring additions and changes to the chart of accounts are complete and accurate.

10. To provide a proper audit trail, **we recommend** that procedures be established requiring supporting documentation to be maintained for all segment value changes to the chart data.

11. **We recommend** that ministries periodically review the cross validation rules defined for their ministry to ensure the rules are set appropriately for their business, allowing proper validation to take place.

Appendix B: Summary of Recommendations

Ensuring chart of accounts remains current and relevant.

12. **We recommend** that monitoring activities be formalized and carried out by Office of the Comptroller General (OCG) to ensure the chart data remains current and relevant.

Journal Processing

Ensuring only valid and authorized journal entries are recorded in the general ledger.

13. Because using the responsibility for inter-ministry journals to enter intra-ministry journals increases the risk of data entry errors, **we recommend** that management evaluates this risk versus the gain in efficiencies.

14. **We recommend**that ministries review their needs and requirements, and determine if they could benefit from the use of recurring or allocation journals to allow for more efficient and effective journal processing.

Ensuring all journal entries are accurate and are posted only once to the general ledger.

15. To ensure that all journal batches are clearly distinguished, **we recommend** that ministries adhere to the established batch naming convention when creating journal batches in Oracle Financials general ledger.

16. **We recommend**that ministries review their journal processing process to ensure proper procedures are in place to prevent duplicate journal entries.

Ensuring all journal entries are posted to the correct reporting period.

No recommendations were required.

Appendix B: Summary of Recommendations

Reconciliation and Financial Reporting

Ensuring all financial statement and account reconciliations are complete, accurate and timely.

17. **We recommend** that a reconciliation procedure be established to provide OCG management with the necessary assurance that the data in CODE is complete, accurate and timely and reflects the data in the Oracle Financials production system.

18. **We recommend** that OCG communicates clearly to ministries the responsibility and requirement for reconciling the liability balance as reported in the Oracle Financials accounts payable subsidiary ledger to the general ledger.

19. **We recommend** that ministries maintain a reconciliation schedule to ensure all accounts are reconciled and to allow management to oversee the month-end reconciliation process.

Ensuring the production and distribution of financial reports is timely.

No recommendations were required.

Supplier Maintenance Controls

Ensuring access to create and change supplier information is appropriately restricted to authorized individuals.

Recommendations included under security administration controls.

Ensuring configurable controls are designed into the process to maintain the integrity of supplier information.

20. **We recommend** that procedures be established to identify suppliers with missing address information, and update them accordingly.

Appendix B: Summary of Recommendations

Ensuring additions and changes to the supplier information are valid, complete, accurate and timely.

21. **We recommend** that procedures be established requiring a copy of the supplier invoice or other documentation supporting the requested change be forwarded to the ministry supplier maintenance person to ensure accuracy and validity of the information entered to the supplier table.

22. **We recommend** that verification procedures be strengthened to include a search on supplier addresses to assist in identifying whether the supplier already exists in the supplier table.

23. To promote effective supplier searches, **we recommend** that Corporate Accounting Services identify and correct all supplier names and addresses of existing records that have not been formatted according to the standard naming and addressing conventions.

24. **We recommend** that Corporate Accounting Services reinforce with ministry staff the importance of following the standard naming convention when entering new supplier information, and verifying the entries to supporting documents for accuracy.

25. **We recommend** that Corporate Accounting Services reinforce with its staff the importance of checking the entered supplier information for compliance and establish periodic review procedures to ensure that the naming and addressing conventions are being complied with.

Ensuring supplier information remains current and relevant.

26. **We recommend** that monitoring activities be established to ensure the supplier data remains current and relevant.

27. To maintain data integrity, **we recommend** that Corporate Accounting Services periodically review the supplier table to identify duplicate suppliers and deactivate them accordingly.

28. **We recommend** that Corporate Accounting Services explore the feasibility of carrying out a data matching process, comparing the supplier information to that of the provincial Corporate Registry, so supplier records can be updated to reflect current information.

29. To facilitate this data matching, **we recommend** that procedures be established to require the collection of the business registration numbers for all new business suppliers, and when practical, for existing business suppliers as well.

30. **We recommend** that Corporate Accounting Services establish formal policies restricting further set-up of generic suppliers and formalize a plan to establish a well-defined approach for using, managing and updating existing generic supplier records.

31. **We recommend** that OCG establish clear policies and guidelines for the ministries, to guide them when using block suppliers in processing payments

32. **We recommend** that OCG establishes clear criteria for monitoring and compliance activities to ensure that the block supplier data remains current and relevant.

33. **We recommend** that an assessment be carried out to identify all high-risk block supplier payment types where the potential exposure of the payee could compromise confidentiality and privacy and appropriate procedures be established to ensure proper processing of these payments with due regard to confidentiality of information.

Ensuring additions and changes to the supplier banking information are valid, complete, accurate and timely.

34. **We recommend** that policies and procedures be established to define clearly the ministry's role and responsibilities in the bank account maintenance process, and to govern the extent of ministry review required for ensuring the completeness and accuracy of banking information obtained.

35. **We recommend** that control procedures be strengthened to ensure accuracy and completeness of bank account change information originated from the supplier, an important measure to ensure authenticity of the supplier.

36. **We recommend** that OCG effectively communicate to the ministries the risks associated with banking activities and advise them of how to detect the potential threats and to ensure that controls are functioning properly to address them.

Ensuring supplier bank information remains current and relevant.

37. **We recommend** that management at Corporate Accounting Services formalize procedures to monitor all supplier linkages to bank accounts and compare the details of the reported link activities to the source documents to ensure that there is no unauthorized or inappropriate bank account linkages.

38. **We recommend** that procedures be established to periodically review the bank account information for suppliers with multiple sites to ensure that they take on the same bank account details on each of their sites.

39. **We recommend** that periodic review procedures be established to ensure that bank accounts that are flagged for single supplier assignment, are only assigned to one supplier.

40. **We recommend** that management determine if retention of electronic payment request forms is required and if so that the required copies are retained in locked cabinets.

Purchasing and Accounts Payable Controls

Ensuring access to create, change, or cancel purchase requisitions, purchase orders and invoices is appropriately restricted to authorized individuals.

41. **We recommend** that access granted to users with expense authorities be reviewed periodically to ensure the Oracle Financials responsibilities assigned to them are compatible with their role as expense authority.

Ensuring Oracle Financials approval levels are secured and configured in conformity with established business requirements.

42. **We recommend** that Corporate Accounting Services determine the feasibility of restricting expense authority administrators to only assigning approval levels to employees within their own ministry.

Appendix B: Summary of Recommendations

43. **We recommend** that ministry expense authority administrators be informed of staff changes at the same time as security administrators, to ensure prompt update of necessary changes to employee approval levels.

44. **We recommend** that monitoring procedures be established to periodically review the setup of the expense authority approval levels in Oracle Financials to ensure that the approval levels assigned to expense authorities remain current and appropriate.

Ensuring payments are only made for authorized purchases, and for goods and services received.

45. **We recommend** that Corporate Accounting Services explores the feasibility of not allowing the expense authorities to approve critical changes that they made directly to a transaction.

46. **We recommend** that ministries reassess their business practices and implement appropriate monitoring activities for detecting and managing non-compliance over the segregation between an expense authority and a receiver.

47. **We recommend** Corporate Accounting Services review the feasibility of distinguishing an expense authority approval versus a non-expense authority action and record them differently in the Oracle tables.

Ensuring key financial reports are reviewed and monitored to ensure validity, completeness and accuracy of recorded transactions.

48. **We recommend** that guidance be established to ensure expense authorities are aware of the risks of manually changing addresses where goods are to be delivered, and that proper validation procedures be carried out approving these changes.

49. **We recommend** that Corporate Accounting Services explore the feasibility of requiring approval from expense authorities when manual changes are made to suppliers' cheque mailing addresses, to prevent unauthorized changes. Guidance should also be established to ensure that proper validation procedures be carried out when approving changes.

Appendix B: Summary of Recommendations

50. **We recommend** that management require expense authorities to review procurement transactions when supplier information is subsequently added to purchase orders or changed, to ensure appropriateness of the suppliers used for procuring the goods and services.

51. **We recommend** that OCG take on the initial responsibility of effectively communicating with ministries the risks of potential fraud in purchase and accounts payable transactions and advising them on how to detect potential threats resulting from these risks.

52. **We recommend** that ministries regularly monitor reports for force-approved transactions to ensure that there are no occurrences and when there are occurrences, all transactions are appropriate and have received proper expense authority approvals.

Appendix C: Office of the Auditor General: 2006 / 2007 Reports Issued to Date

Report 1 - April 2006

Strengthening Public Accountability: A Journey on a Road that Never Ends

Report 2 - October 2006

The 2010 Olympic and Paralympic Winter Games: A Review of Estimates Related to the Province's Commitments

Report 3 - November 2006

Treaty Negotiations in British Columbia: An Assessment of the Effectiveness of British Columbia's Management and Administrative Processes

Report 4 - December 2006

Province of British Columbia Audit Committees: Doing the Right Things

Report 5 - December 2006

Audit of Government's Corporate Accounting System: Part 2

Each of these reports can be accessed through our website http://www.bcauditor.com or requested in print from our office.